(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SYSTEM EVALUATION OF A FREQUENCY
HOPPING COMBAT NET RADIO

by

Syed Agha Hussain

September 1991

Thesis Advisor: Dan C. Boger

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution is unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION: Naval Postgraduate School; 6b OFFICE SYMBOL (If applicable): Code EW	7a NAME OF MONITORING ORGANIZATION: Naval Postgraduate School
6c ADDRESS (City, State, and ZIP Code): Monterey, CA 93943-5000	7b ADDRESS (City, State, and ZIP Code): Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION; 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS: PROGRAM ELEMENT NO; PROJECT NO; TASK NO; WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

SYSTEM EVALUATION OF A FREQUENCY HOPPING COMBAT NET RADIO

12 PERSONAL AUTHOR(S)

Hussain, Syed Agha

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM ____ TO ____	1991 September	90

16 SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Spread Spectrum, Frequency Hopping, Anti-Jamming, System Evaluation, ECCM, EW, CNR

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The importance of survivable radio communications in contemporary EW threat environments cannot be overemphasized. At the tactical level, in fast and fluid conditions, radio will remain the primary means of communication for command and control. Thus, it will be subjected to hostile EW efforts, e.g., jamming, direction finding, interception, etc. Therefore, the aim of this thesis is to carry out a comparative evaluation of several state-of-the-art frequency hopping combat net radios in order to select the best available choice for fielding into the Pakistan Army. The methodology of evaluation is primarily based on the system specifications provided by respective vendors. Greater emphasis is laid on the anti-jamming performance and upgradability of the systems in the process of evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT: ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION: Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL: Dan C. Boger	22b TELEPHONE (Include Area Code): (408) 646-2607; 22c OFFICE SYMBOL: AS/Bo

DD Form 1473, JUN 86 Previous editions are obsolete SECURITY CLASSIFICATION OF THIS PAGE Unclassified

S/N 0102-LF-014-6603

Approved for public release; distribution is unlimited.

System Evaluation of a Frequency Hopping Combat Net Radio

by

Syed Agha Hussain
Major, Pakistan Army
B.E., UE&T, Lahore, 1983

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Author: ______________________
Syed Agha Hussain

Approved By: ______________________
Dan C. Boger, Thesis Advisor

____
Allan Tulloch, Second Reader

____
Joseph Sternberg, Chairman
Electronic Warfare Academic Group

ABSTRACT

The importance of survivable radio communications in contemporary EW threat environments cannot be overemphasized. At the tactical level, in fast and fluid conditions, radio will remain the primary means of communication for command and control. Thus, it will be subjected to hostile EW efforts, e.g., jamming, direction finding, interception, etc. Therefore, the aim of this thesis is to carry out a comparative evaluation of several state-of-the-art frequency hopping combat net radios in order to select the best available choice for fielding into the Pakistan Army. The methodology of evaluation is primarily based on the system specifications provided by respective vendors. Greater emphasis is laid on the anti-jamming performance and upgradability of the systems in the process of evaluation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

Test and evaluation (T&E) of a military system is an important step in the acquisition process which must be taken with extreme caution and circumspection. It should begin as early as in the system developmental stage and should continue concurrently, step by step, until the system is finally approved and inducted. The design and execution of a sound test plan is no accident. It requires thorough understanding of testing techniques, the system under test, its operating scenario, and above all, the honest and numerous restless hours of hard work. The principal objective of T&E is to reduce acquisition risk and provide insight into the system's performance to meet the required operational capability (ROC). It also enables the acquiring organization to know the system's inherited flaws, which may be eliminated or improved upon by devising changes in tactics and doctrine.

The objectives of this thesis are:

1. To describe the spread spectrum techniques.

2. To carry out comparative evaluation of the state-of-the-art frequency hopping combat net radio (CNR) systems based on the vendors' specifications.

3. To highlight broad guidelines for operation, test, and evaluation (OT&E) / field trials of a system.

In pursuit of acquiring systems data, letters were written to six world famous companies that manufacture frequency hopping CNR systems. Appendix A lists the names and addresses of the companies approached.

Chapter II is aimed at emphasizing the need for ECM-hardened and survivable combat communication systems. It also highlights the salient features and attributes of spread spectrum (SS) systems, mainly the electronic counter-countermeasures.

Chapter III deals with the development of the required theoretical knowledge of SS techniques. For this chapter, a working background knowledge of digital communication and signal processing is recommended.

Chapter IV briefly discusses radio communication concepts at the tactical level. It also presents requirements of a typical CNR system for combat communication.

Chapter V covers system evaluation, using both the techniques mentioned before. It also integrates most of the theoretical concepts of the prior chapters into practice. Some of the limitations of this thesis work are enumerated here.

Chapter VI presents conclusions and recommendations. The recommendations and conclusions are mostly based on the objective analysis from Chapter V.

II. BACKGROUND

A. COMBAT COMMUNICATION AND ELECTRONIC WARFARE

Command, control, and communications play an extremely pivotal role in employing overall combat power in the contemporary battlefield which is saturated with all kinds of highly mobile, lethal, and destructive arsenals. Of all the available means of communication at the tactical level, radio has shown tremendous promise due to its inherent characteristics such as flexibility, mobility, speed, and cost effectiveness. However, its serious disadvantage is its vulnerability to the enemy electronic warfare (EW) threat, namely interception, monitoring, direction finding (DF), and jamming. Hence, radio communication, by doctrine, remains secondary to other means of communication such as line, radio relay (RR), satellite and message carrying agencies.

Nevertheless, at tactical levels in all mobile operations of war, radio remains the primary means of communication available to a battalion, brigade, or division commander. Amidst the enemy EW capabilities viz-a-viz the versatility of radio communication, a tough challenge has been posed to a designer or operator. This challenge is to make friendly radio signals covert and anti-jam (AJ), thereby defeating or suppressing enemy effects of electronic countermeasures (ECM).

The branch of EW that enables the friendly use of the electromagnetic spectrum despite enemy active ECM is called electronic counter-countermeasures (ECCM). Some of the electronic counter-countermeasures used are as follows: [Ref. 1]

1. Spread spectrum (SS) communication.
2. Error control coding (ECC).
3. Null steering antennas.
4. Power management:
    a. Turn radio transmitter off (emission control).
    b. Vary transmitter's effective radiated power (ERP).
5. Alternate route transmission.
6. Dial tone transmission or burst transmission.
7. Mobility (non electronic).
8. Frequency management.

While there is no guaranteed technique that is perfectly covert or jamproof, laser beam communication ranks very high on the ECCM ladder. However, owing to its point-to-point short range and less flexible nature, it is limited to only specific applications. On the other hand, SS communication systems, having greater flexibility, have proved very effective and are widely used in ECM environments. Appendix B shows some of the likely EW threats and possible solutions.

B. SALIENT FEATURES OF SPREAD SPECTRUM SYSTEM

Some of the salient features of modern SS systems are as follows: [Ref. 2]

1. The carrier is made unpredictable by using a pseudo-random wideband signal.
2. The bandwidth of the carrier is made much wider than the bandwidth of the data or information.
3. Reception is accomplished by cross correlation of the received wideband signal with a synchronously generated replica of the wideband carrier.

C. SPREAD SPECTRUM SYSTEM ATTRIBUTES

SS systems, because of their signal power spreading, have the following important attributes: [Ref. 1]

1. Low Probability of Intercept (LPI) can be achieved with high processing gain and unpredictable carrier signal with power being thinly spread below the noise floor. A low probability of position fix (LPPF) goes a step further encompassing both intercept and DFing. Low probability of signal exploitation (LPE) may include some additional features. [Ref. 3]

2. Antijam Capability can be achieved to a greater extent by using an unpredictable carrier signal. The greater the unpredictability and less response time offered to the jammer, the less the chances of jamming. However, partial band jamming and repeat jamming, depending on enemy EW capabilities, may pose concerns under certain circumstances.

3. High Time Resolution is attained by the correlation detection of wideband signals. Differences in the time of

arrival (TOA) on the order of the reciprocal of the signal bandwidth are detectible. This property can be used to suppress multipath, and by the same token, render a repeat jammer ineffective.

4. A number of transmitters and receivers can operate in the same bandwidth employing different pseudorandom noise (PN) codes. Such systems are called SS <u>Code Division Multiple Access (CDMA) systems.</u>

5. <u>Message Privacy</u> is inherent in SS signals because the data modulation cannot be distinguished from the carrier, and the carrier modulation is effectively random to an unintended receiver.

6. <u>Selective Addressing</u> is possible by using different codes assigned in a network. A transmitter can select any one of the receivers by simply transmitting its code, and that receiver will receive the message.

III. SPREAD SPECTRUM COMMUNICATION OVERVIEW

A. GENERAL

A spread spectrum system is defined as a system in which the transmitted signal is spread over a wider frequency band, much wider, in fact, than the minimum bandwidth required to transmit the information being sent.

SS systems employ any one or a combination of the following techniques:

1. Direct Sequence or Direct Spreading (DS).
2. Frequency Hopping (FH).
3. Time Hopping (TH).
4. Chirping.
5. Hybrid.

B. DESCRIPTION OF SPREAD SPECTRUM TECHNIQUES

1. Direct Sequence Spread Spectrum (DSSS)

Direct sequence signals are generated by modulating the carrier with a pseudorandom code sequence.
The DSSS signal varying envelope: [Ref. 3]

$$s(t) = A * c(t) * \cos \{ wt + O(t) \} \quad \text{-------------(1)}$$

where A = amplitude of carrier, c(t) = PN spreading code, w=frequency of the carrier, and O(t) = phase angle.

DSSS is similar to a conventional amplitude modulated (AM) or frequency modulated (FM) communication link with code modulation laid on the carrier. The simplest form of DSSS transmitter employs Biphase Phase Shift Keying (BPSK) as the spreading modulation and is shown in Figure 1 [Ref. 3].

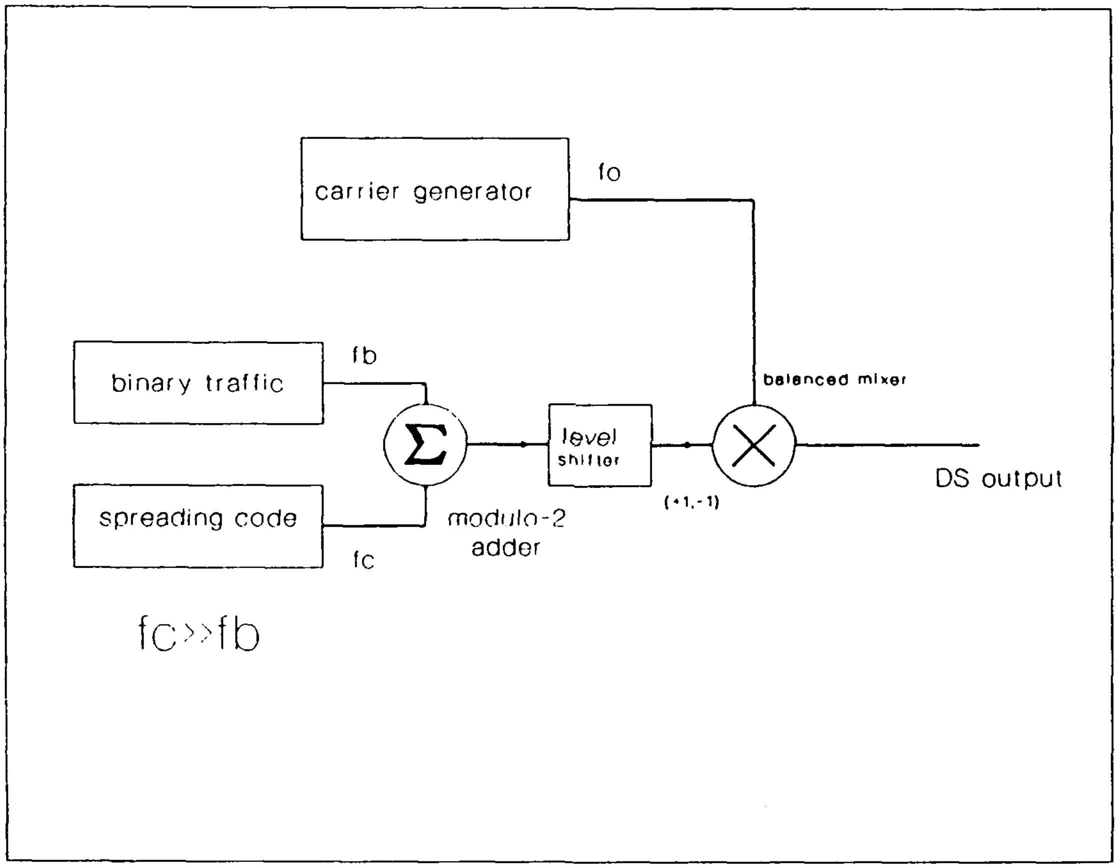


Figure 1

Block Diagram Of DSSS Transmitter [Ref. 3]

As shown, the carrier is not usually modulated directly by a baseband information signal. Rather, the incoming information signal, if not in data form, is first digitized, then modulo-2 added to a higher speed PN sequence. The modulation is performed by any fast acting analog multiplier (a balanced modulator). The bandwidth of the modulated envelope is mainly determined by high speed code sequence responsible to produce an SS signal. The ideal BPSK modulation causes 180 degrees instantaneous phase shift of the carrier, implying multiplication of s(t) by +1 and -1. Figure 2 [Ref. 3] illustrates implementation of Figure 1 and the resultant waveforms of a DSSS signal.

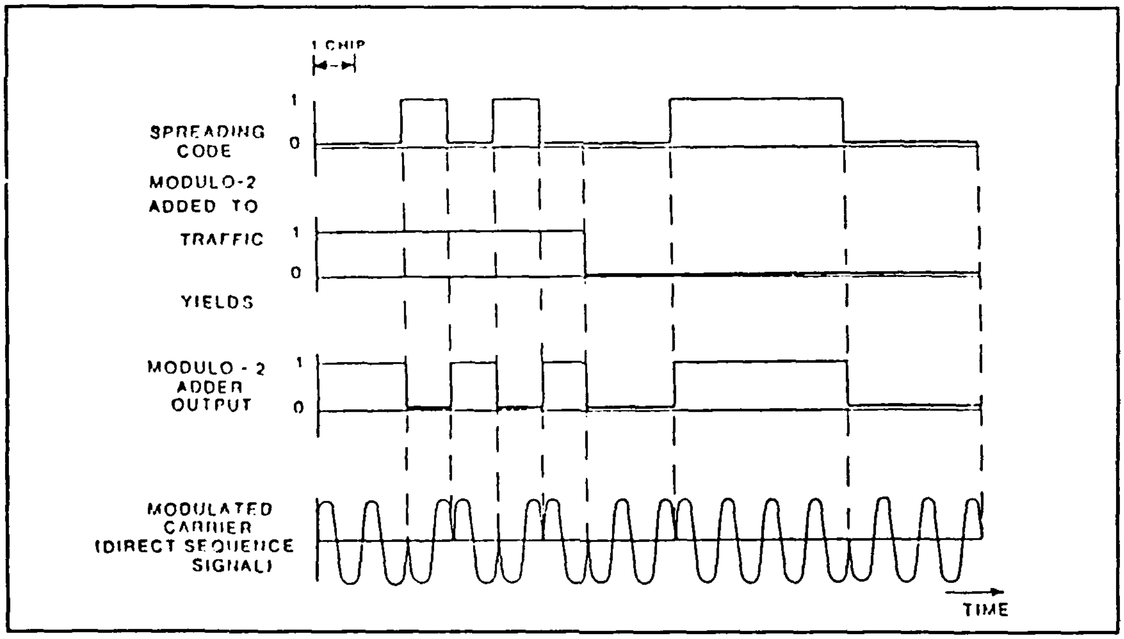


Figure 2
Generation of DS Spread Spectrum Signals [Ref. 3]

The DSSS received signal along with some type of added noise, after suffering transmission delay (Td), is demodulated by the receiver. The correlation of the synchronous PN code with the incoming signal will despread the signal as shown in Figure 3 [Ref. 3].

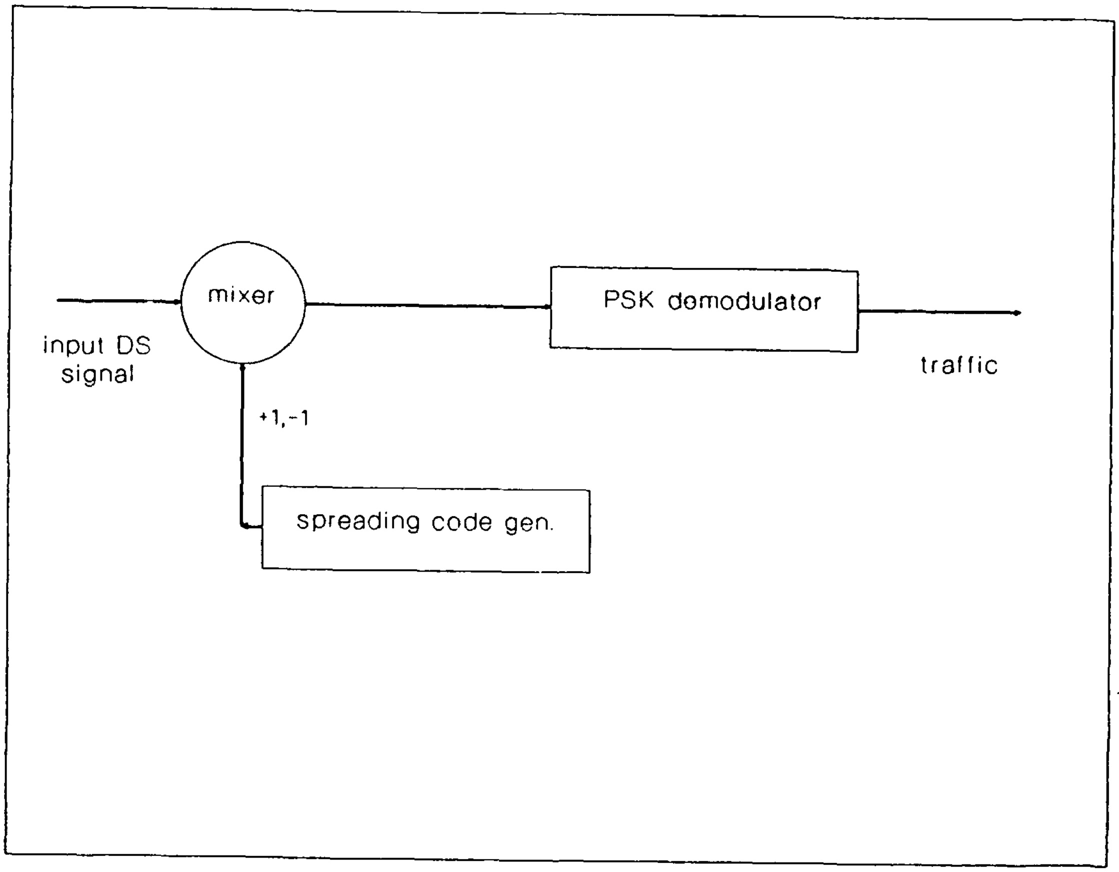


Figure 3

Block Diagram of DSSS Receiver [Ref. 3]

Use of Quadraphase Phase Shift Keying (QPSK) modulation, although more complex, will have principal advantages of increased covertness and more immunity to jamming. The QPSK DSSS signal can be mathematically expressed as: [Ref. 4]

s(t)= A1*c1(t)cos(wt+O(t))+A2*c2(t)sin(wt+O(t)) ----(2)

where c1 and c2 are two quadrature carriers with amplitudes A1 and A2. The block diagrams of the QPSK transmitter and receiver are shown in Figure 4a and 4b [Ref. 4].

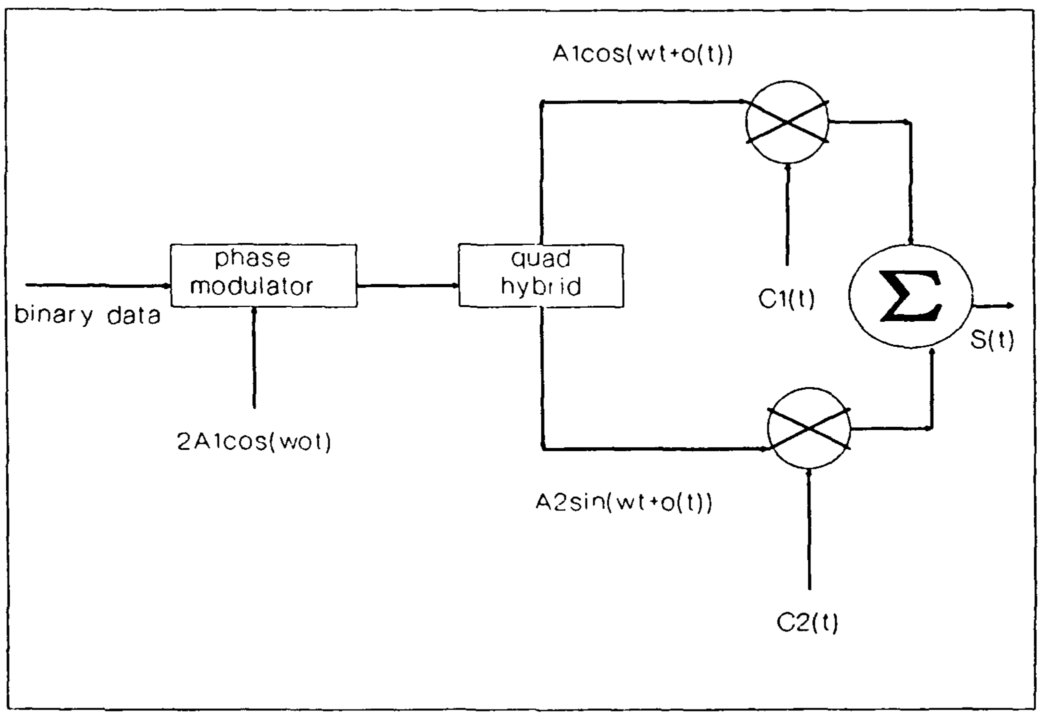


Figure 4a

QPSK SS Transmitter [Ref. 4]

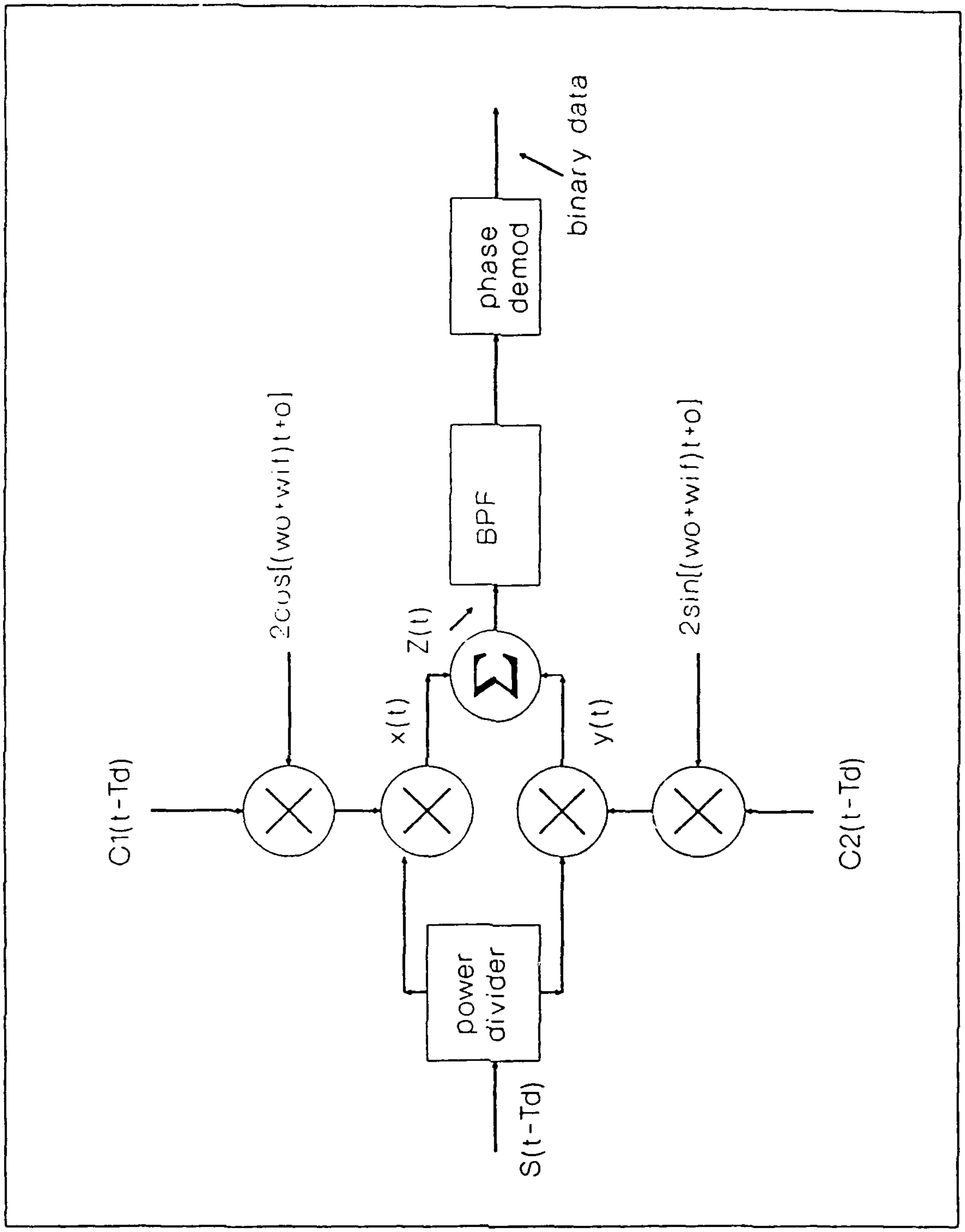


Figure 4b

QPSK SS Receiver [Ref. 4]

2. Frequency Hopping

Frequency hopping (FH) SS systems are frequency-agile systems in which a very large RF bandwidth is generated by changing the carrier frequency pattern over a wide range of frequencies. The most general frequency hopped RF signal is of the form: [Ref. 5]

$$s(t) = A \cos \{2*pi*f(t)\} \quad \text{--------------------}(3)$$

The function f(t), which describes the carrier frequency as a function of time, determines the hopping pattern and produces the FH signal. To provide privacy of information, the hopping pattern is made unpredictable by switching the frequency of the synthesizer using a pseudorandom sequence. The technique, therefore, may also be called "multiple frequency, code-selected, frequency shift keying."

A simplified block diagram of a FH SS system is shown in Figures 5a and 5b [Ref. 4]. Any of the PN code k chip words is taken randomly to determine one particular frequency to be mixed with the modulated bandwidth out of 2^k available hop frequencies. Change in chip word per second is actually the hopping rate, which in conjunction with the number of available frequency choices, are two very important design parameters. For most of the practical systems, the discrete frequencies available should be typically on the order of 2^{20}.

For fast FH systems, the hopping rate is much higher than the data rate and will provide much greater band spreading as compared to a slow FH system in which the hopping rate is smaller than the data rate. Figure 6 [Ref. 3] illustrates the fast and slow hopping signal waveforms.

As a result of greater signal spreading, which in turn buries the signal much below the noise floor, the probability of unintended detection and subsequent jamming of the signal

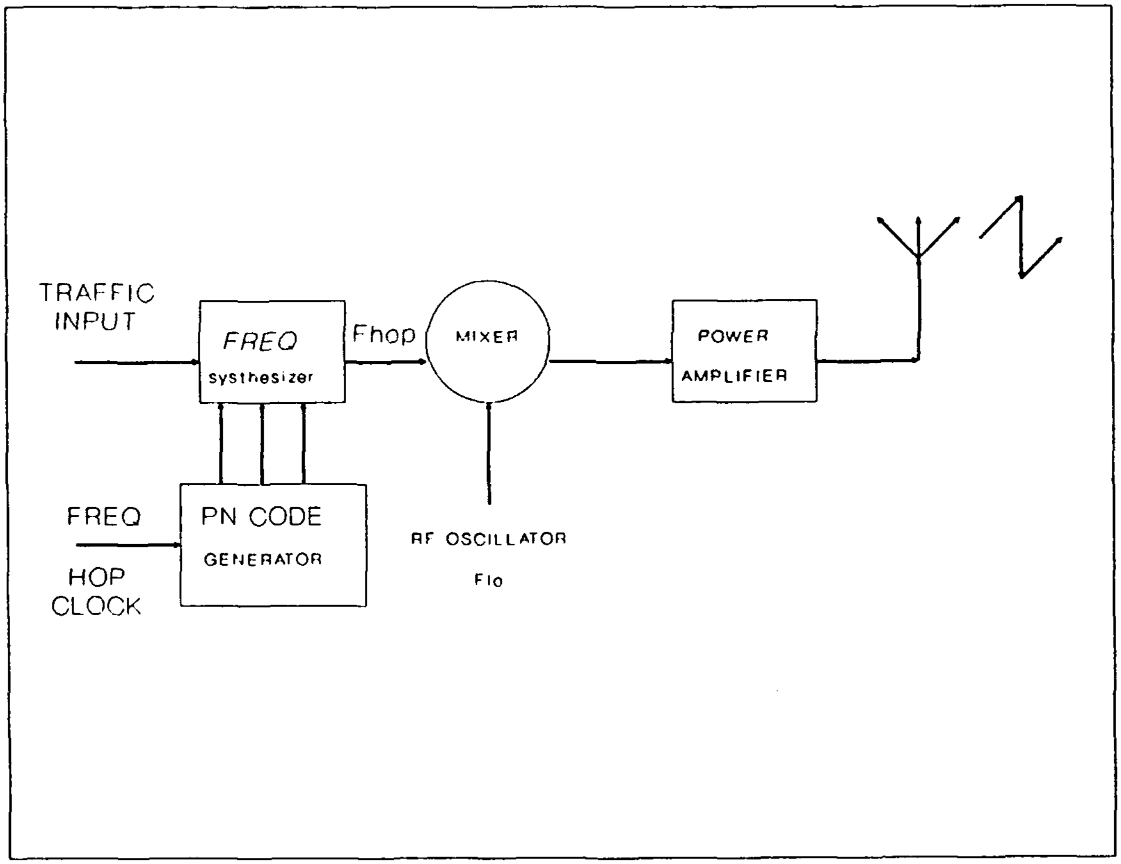


Figure 5a

FH Transmitter [Ref. 4]

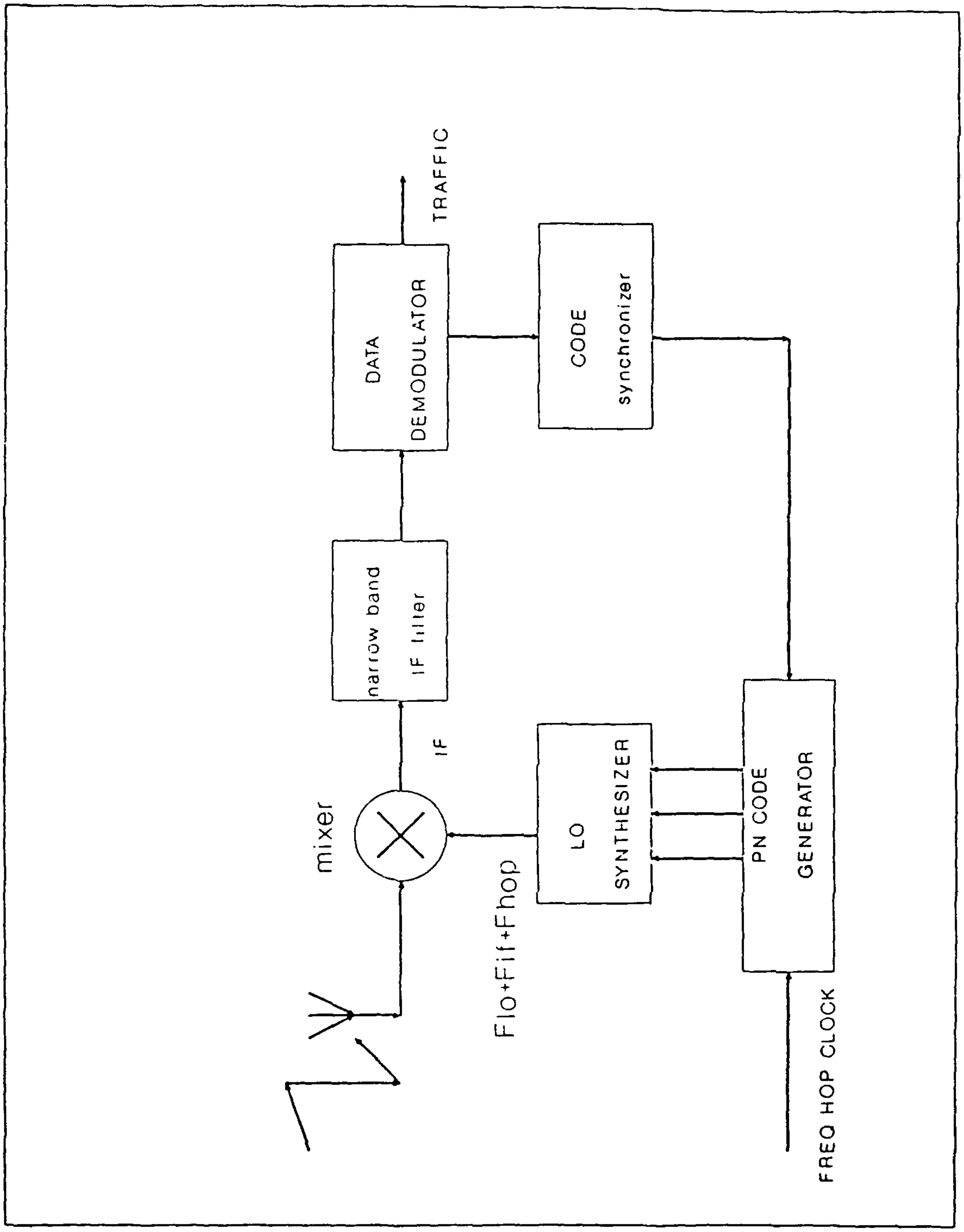


Figure 5b

Receive Freq Hop Demodulator [Ref. 4]

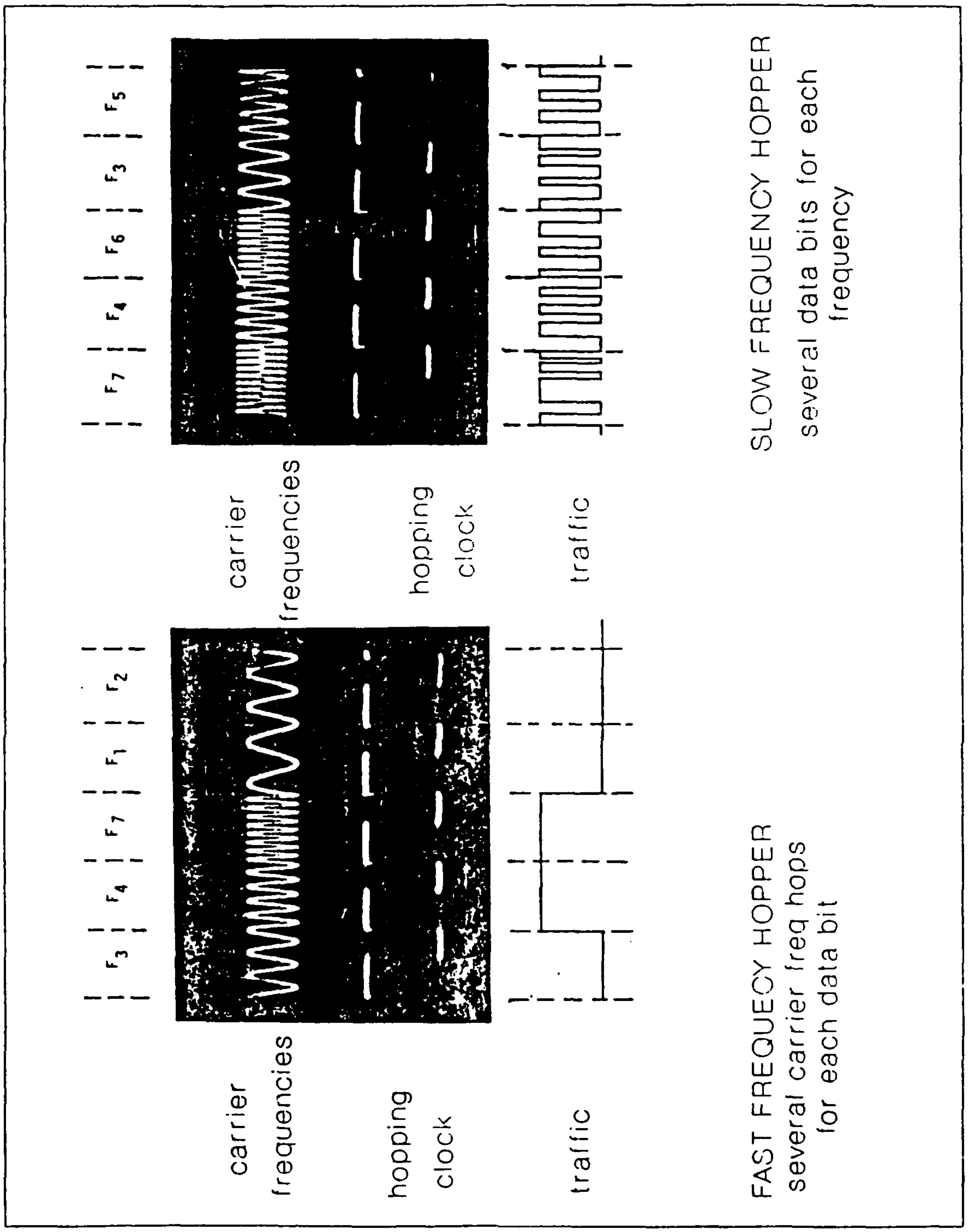


Figure 6

Comparison Of Fast and Slow FH System Waveforms [Ref. 3]

becomes difficult. Hence, fast FH systems are more immune to partial band jamming and repeat jamming. Also, using a non-coherent / differentially coherent data modulation scheme makes FH SS comparatively simple (based on synchronization), economical, and one of the favorite choices for military communications.

3. Time Hopping Spread Spectrum System

Time hopping (TH) spread spectrum modulation, identical to pulse modulation, switches the transmitter on and off using a pseudorandom code sequence. In TH, the message bit may be divided into a number of nonoverlapping subintervals. One of the subintervals is selected pseudorandomly in each bit interval, and a pulse is transmitted that conveys the value of the bit. The subinterval selected is independent of the bit value and is independent bit-to-bit. In a sense, TH uses time slots, or subintervals, in a way that is analogous to the manner FH uses frequency cells. Figure 7 [Ref. 2] shows a block diagram of time-hopping system.

The time hopping system is relatively more vulnerable to jamming as the signal may be interfered with by a determined jammer, keeping his transmitter continuously on at the carrier frequency. Therefore, simple TH is not used in ECCM applications but rather is combined with other systems such as FH. Some applications of TH are found in the areas of ranging and multiple access.

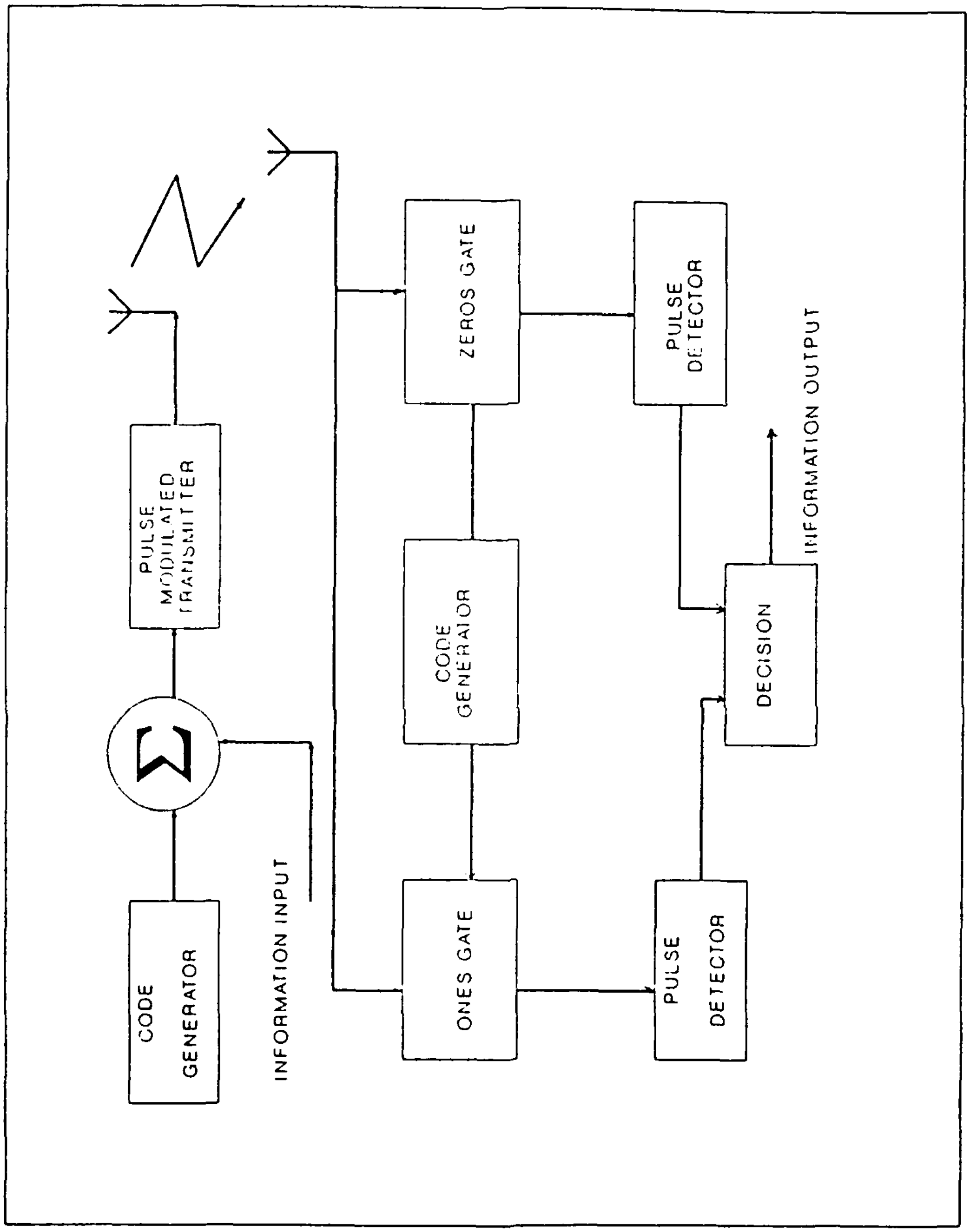


Figure 7

Simple Time Hopping System [Ref. 2]

4. Hybrid Spread Spectrum System

To get the advantages of any two or more types of systems, most of the state of the art SS systems use a hybrid (combination) configuration. The hybrid systems provide greater jamming immunity and enhanced covertness. The most common combinations used in SS systems are: [Ref. 2]

1. Frequency Hopping - DS System.
2. Time Hopping - DS system.
3. Time - Frequency Hopping.

5. Chirp Spread Spectrum System

Chirp SS systems mostly employ linear frequency modulation (FM) in which the carrier frequency is varied in a specifically pre-determined way using a typical ramp impulse. This technique is commonly used in radar systems; however, it can be very useful in communication systems too. A typical simplified block diagram of a chirp signal generator which utilizes a voltage controlled oscillator (VCO) to produce varying carrier frequencies is shown in Figure 8 [Ref. 3]. The information input, represented by marks and spaces (M and S), is converted into a ramp waveform. These ramp voltages are used to control the frequency of a VCO. The output of the VCO is the chirp signal which is then mixed with a LO output in order to translate it to a required transmission frequency. [Ref. 3]

The receiver in this system uses a matched filter, matched to the angular rate of change of the transmitted

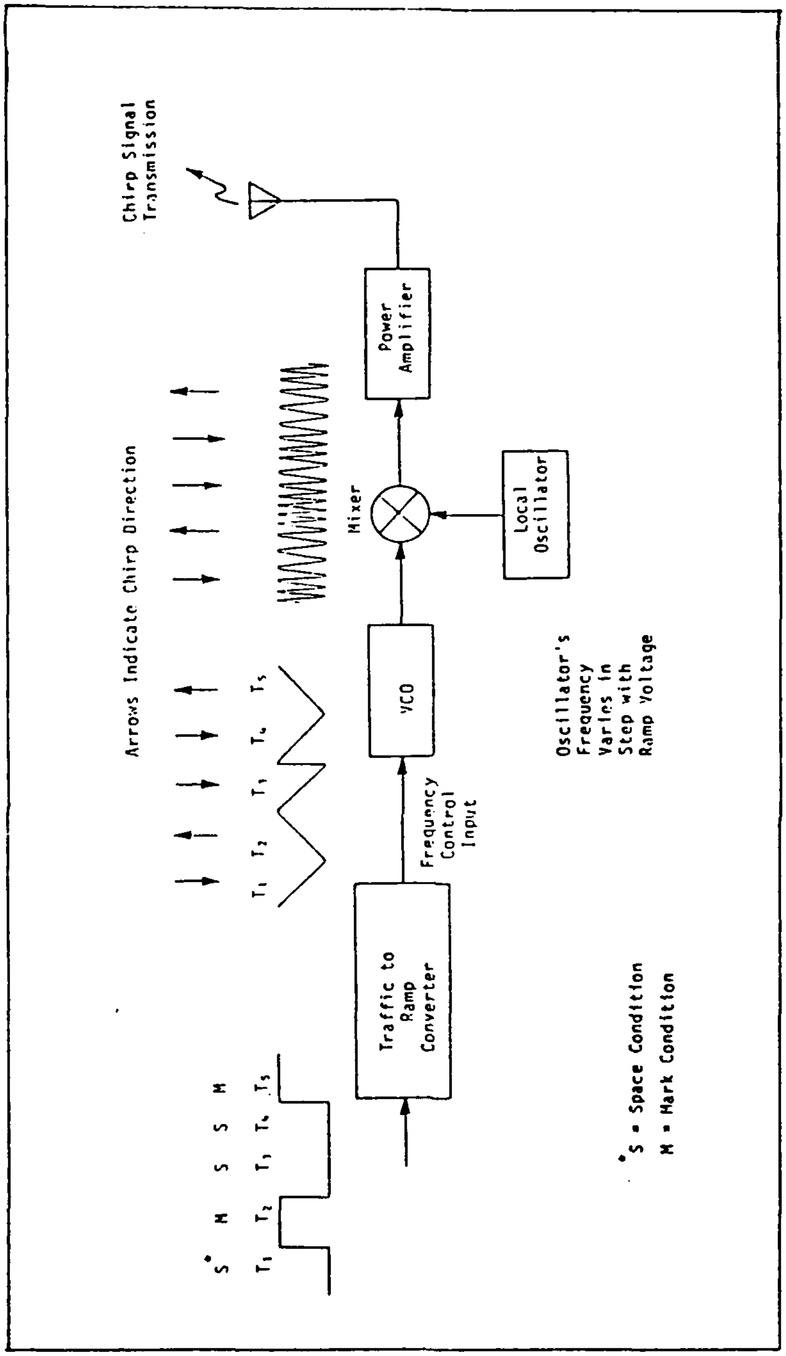


Figure 8

Block Diagram Of a Typical Chirp Signal Generator

frequency-swept signal. Chirp systems using non-linear frequency modulation would pose greater difficulty to the enemy with regards to signal analysis and demodulation. This feature of the chirp system would make it a very good candidate for ECCM applications.

C. COMPARISON OF SPREAD SPECTRUM TECHNIQUES

1. Frequency Hopping (FH) and Direct Sequence (DS)

a. Since the instantaneous power density of FH is more than when using a DS system, its LPI performance is not as good as that of a DS system.

b. DS has better multipath performance provided the multipath delays are larger than the DS chip duration ($1/f_c$).

c. Co-siting of FH is easily solved by good frequency management and synchronous technique as FH does not suffer from the Near/Far problem.

d. Modern digital technology and field-proven experience with FH are mature enough to produce an effective and jamming immune tactical radio system at a reasonable cost.

e. Most of the components of an FH radio are identical to those of a conventional radio set. This makes FH more suitable for implementation as an add-on feature to existing VHF radios.

2. Hybrid and FH / DS

a. Hybrid systems share both advantages and disadvantages of FH and DS techniques. Hybrid techniques are employed in the following applications:

(1) When higher processing gain is needed but unobtainable by using a single technique.

(2) When improved LPI performance is essential.

(3) When it is required to overcome severe multipath effects.

(4) When no co-siting restrictions are imposed.

b. The LPI and multipath performance of hybrid systems have a greater promise than FH systems provided the co-siting requirement is not taken into consideration or the future technology provides solution.

3. How to Select the FH Technique for Military Tactical Communication?

Radio communication at the tactical level is based on multiple nets. In a division scenario, about 200 nets operate in an area. The principal disadvantages of DS systems as mentioned earlier are the Far / Near problem and reduced number of available channels. For a low jamming margin, e.g., 12 dB or less, a nearby interfering transmitter located at half the range of the desired transmitter will prevent effective communication completely. Therefore, for a tactical radio system, using DS, code division multiplexing (CDMA) cannot be used. This implies that the number of nets sharing the same frequency in the same area is virtually limited to ONE only. Hence, the two problems, co-location and the reduced number of available channels, are enough to preclude the use of DS techniques in multiple net communication. The FH systems have more available channels, hence, high processing gain, and no co-location problem if frequency management and synchronization is taken care of. Good algorithms practically used show that the latter requirements are fulfilled with a greater degree of confidence.

IV. CONCEPT AND REQUIREMENT OF RADIO COMMUNICATION AT THE TACTICAL LEVEL

A. CONCEPT OF RADIO COMMUNICATION AT THE TACTICAL LEVEL

Radio is used very sparingly owing to its vulnerability to the enemy EW threat. In all defensive operations of war (except for counterattack and counterpenetration phases), radio remains a secondary or standby means of communication. However, in all offensive operations where movement of troops takes place, radio takes over as a primary means of communication.

At the tactical level, especially for command and control, radio is used in the form of a network. In a network, basically a number of subordinate headquarters constitute substations and the respective superior headquarters assumes a control station function operating on the same frequency. A typical infantry battalion radio network is illustrated in Figure 9 (down to platoon level).

B. MODERN BATTLEFIELD TACTICAL RADIO SYSTEM REQUIREMENTS

Over the past few decades, the popular VHF band has been sufficiently crowded due to the ever-increasing demand of tactical communications. On the other hand, in response to it, EW activities have also been intensified posing a challenge for a contemporary system to operate optimally.

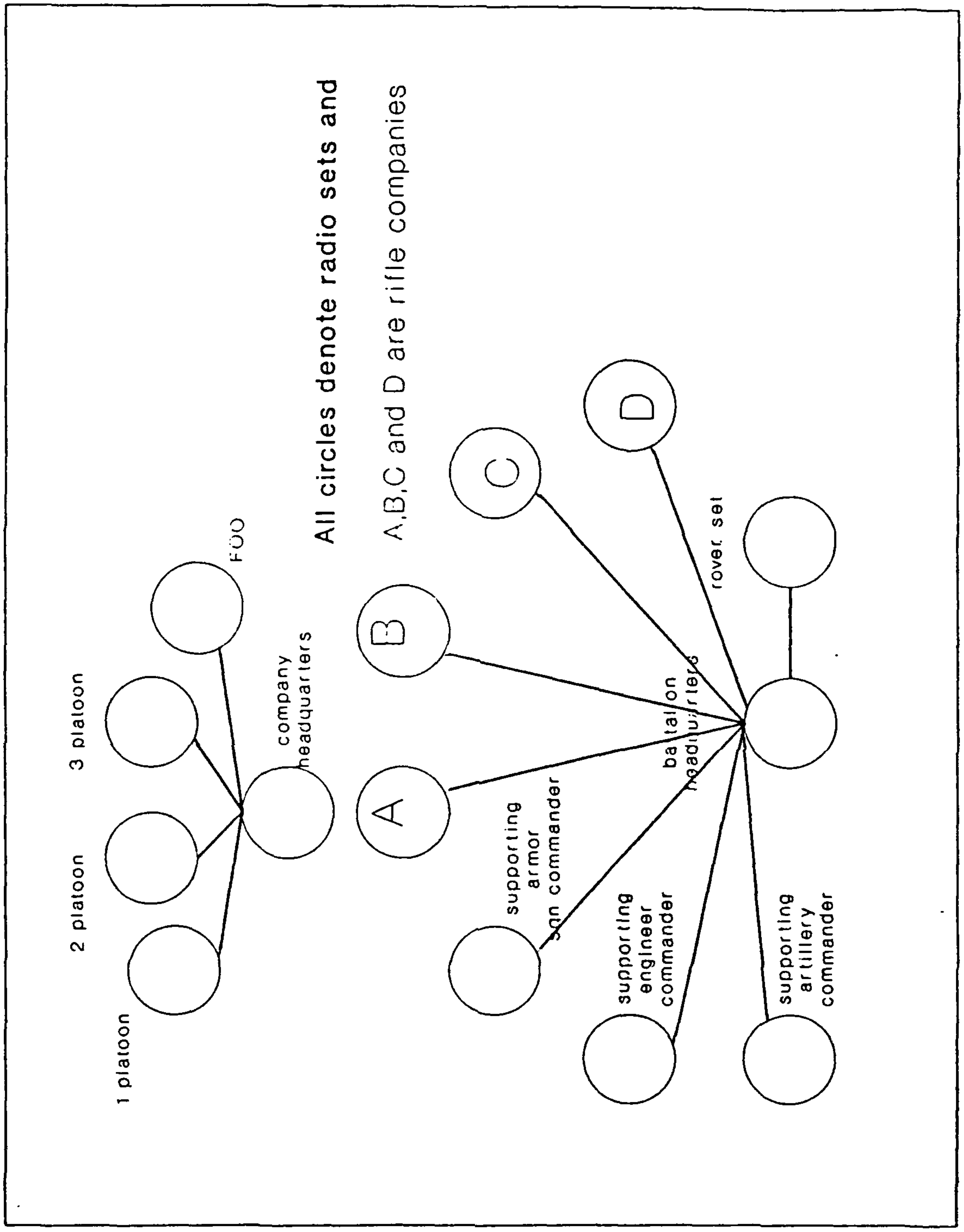


Figure 9

Typical Battalion Command Radio Net Diagram

Following are some of the requirements of a tactical CNR with variations applicable to a specific adversary's capabilities:

1. Covertness / transmission security employing ECCM techniques.

2. Communication security using digital codes.

3. Built-in error detection and correction codes.

4. Highly selective filtering in order to avoid co-siting problem.

5. Simplicity of operation and training. No complicated and time-consuming procedures in use; emphasis rather on automation.

6. Cost effectiveness.

7. High inherent reliability and maintainability.

8. Prolonged operational life cycle.

9. Adding-on / upgradability of special features like anti-jam (ECCM), encryption, burst and data transmission, etc.

10. Easy transportability.

11. Configurability in various versions; hand-held, man-pack, vehicular (both wheeled and track vehicles) and airborne.

12. Power manageability; capable of selecting transmitter power output commensurate to the prevailing scenario.

13. Remote controllability.

14. Automatic retransmission.

V. SYSTEM EVALUATION

A. SCENARIO AND APPROACH

Based on the importance of command, control and communications (c^3), and keeping enemy capabilities in mind, military field commanders recommend the purchase of state-of-the art SS communication systems. The DOD of Pakistan, after thorough deliberations, has approved such proposals, and hence, the defense acquisition and procurement department in turn has approached various companies which manufacture SS systems worldwide. The companies in reply send promotional brochures along with the system specifications. Of these brochures, a comparative evaluation is done so that the authorities can be more selective of the available systems by choosing the systems which fulfilled the requirements. The selected companies are notified accordingly to present the systems for demonstration and subsequent field trials. The demonstrations, when conducted, are to be watched keenly by concerned authorities and the key features of system performance are noted.

The next step is to take the equipment into the local area and conduct field trials. The T&E is done based on the guidelines as given in the ensuing dendritic form (refer to Figures 11-15).

The last step of T&E is to carry out T&E in the most realistic field and environmental conditions by the user organization (infantry, artillery, armour and engineers regiments) duly assisted by the Corps of Signals. These tests are conducted country-wide, preferably under simulated combat conditions or during field training exercises.

The final and the most crucial step is to compile and integrate all of the test results, carry out analytical study, and submit recommendations for command decision. The priority of induction is decided based on these recommendations, and the entire acquisition plan is presented for final approval. The final approving authority is duly assisted by the respective area advisors in reaching the decision of selecting a particular system. Once the system selection has been made, the acquisition and procurement process commences following the procedural activities.

B. SYSTEM EVALUATION METHODOLOGY

For this thesis work, system evaluation is performed using two methods: field trials (OT&E) and system comparative evaluation based on vendor's / contractor's specifications. The former method is kept limited and is aimed at providing broad guidelines for more meticulous and detailed study. Each of these methods is explained in the subsequent paragraphs.

C. SYSTEM EVALUATION BY COMPARISON OF VENDOR'S SPECIFICATIONS

1. General

The approach to system evaluation using the comparison method is to determine the most suitable system for induction into a military organization. The evaluation methodology is based on the different types of specifications, e.g., technical, operational, environmental, etc. Each of the important system specifications is assigned a point value ranging from 0 to 1 and a weight depending on its significance. The quality of a system is determined by summing up the total number of points after being multiplied by the appropriate weighting factor. Hence, relative superiority of a system is found by comparing the individual total grade points. For this work, those parameters that are closely related to ECCM performance of the system are heavily weighted. Extra credit is awarded to the system for additional capabilities, e.g., upgradability (add-on facility), multi-channel carrier and data communication equipment interface, etc.

The fundamental limitation in this method is that it is dependent on the system parameters provided by the manufacturer and cannot be confirmed for accuracy without the follow-on field evaluation. This step in evaluation therefore, must always be followed by laboratory testing and field trials. For this thesis work, it is important to note that the potential adversary's EW capabilities could not be spelled out. However, to remain on the safe side, the evaluation is based on the assumption that the system has to work in the adequately dense contemporary EW environments, particularly with regard to all types of jamming.

2. Evaluation Criteria / Measure of Effectiveness

This section will describe the various measures used to rate the systems and will show the point value for each criterion.

a. General Characteristics

(1) Frequency coverage. It is based on the existing military VHF frequency band which is 30 - 88 MHz:

Full coverage = 1.0

Partial coverage = 0.5 - 0.0

(2) Number of available channels. It is based on the maximum number of available channels with 25 KHz channel spacing:

Over 2000 = 1.0

Less than 2000 = 0.5 - 0.0

(3) Modes of operation. The various modes are CLEAR, COMSEC, ECCM:

Depending on usefulness and variety of modes = 0.0 - 1.0

(4) Power Source. Compatible with existing mains, vehicular and rechargeable batteries = 1.0

Special / unique (simple) = 0.75

Complex = 0.5 - 0.0

(5) Power Output. Relative consideration for long, medium and short range is based on tactical deployment at brigade level. The underlined principle is to use minimum required power for a desired range of communication:

Variable, 3 or more than 3 alternatives = 1.0

Variable, less than 3 alternatives = 0.5 - 0.25

Fixed = 0.0

(6) Combat Net Radio (CNR). Based on the brigade / battalion level tactical scenario where a new station can enter any of the operating nets:

7 or more than 7 memorized nets = 1.0

Less than 7 = 0.5 - 0.0

(7) Remote Control Operation. Remote control operation is determined on the basis of the level of head-quarters being supported and the type of enemy artillery fire:

On field wire with remote control unit (RCU) up to and more than 1.5 KM = 1.0

500 meters to 1.5 KM = 0.5 - 0.25

No remote control facility = 0.0

(8) Automatic retransmission. This facility extends the range of communication and is extremely useful in mountainous terrain where, at places, the signal strength is significantly degraded due to intervening land features:

Provision exists = 1.0

Does not exist = 0.0

b. Anti-jam / ECCM Performance

(1) Hopping Rate. The higher the hopping rate, the more resistant the system is to enemy EW efforts aimed at signal exploitation:

Medium to fast = 1.0

Medium = 0.75

Slow to medium = 0.5

Slow = 0.0

(2) Number of preset channels. While working in the normal mode, or especially in a net having a mixture of FH and other compatible transceivers, preset channels would enable rapid change of frequency in case of jamming:

10 or more = 1.0

less than 10 = 0.5 - 0.0

(3) Number of pre-set frequency tables. Frequency changes follow a pseudorandom pattern within a specific, preset table, but many preset tables would provide additional redundancy and security to the hopping pattern, thereby keeping the enemy busy guessing and correlating the end points of a specific maximal code sequence:

10 or more = 1.0

Less than 10 = 0.5 - 0.0

(4) Synchronization. Synchronization of a transmitter and distant end receiver is key for any FH system to work. Related to human factors, it is essential that

synchronization must be performed conveniently and with minimum loss of time:

Automatic = 1.0

Semi-automatic = 0.5

Manual = 0.0

(5) Orthogonality. This is a performance measure in CNR, when several sub-stations in one net operate in the presence of many nets typically at the tactical level using same frequency table:

4 sets of over 50 or more orthogonal nets over any frequency table = 1.0

Less than 4 sets of over 50 orthogonal nets = 0.5 to 0.0

(6) Loading of keys / frequency plans.

(a) Speed and Ease in Loading.

Automatic = 1.0

Semi-automatic and Manual = 0.5 - 0.0

(b) Transmission Security of Keys.

Using secure transmission built-in system = 1.0

Through other arranged means = 0.5 - 0.0

(7) Erasing of keys. To prevent system compromise in case of capture by the enemy:

Depending on time delay to erase / physically destroy the keys = 0.0 - 1.0

(8) Free Channel Search. To make communication possible even in the presence of enemy barrage jamming, the Free Channel Search (FCS) feature is extremely important. The system in this mode will automatically scan, search, and select a frequency free of jamming. However, this very feature must always be considered along with the enemy capabilities of Direction Finding.

Does FCS exists? Yes = 1.0 No = 0.0

c. Communication Security

The system's capability to maintain the security of information in case of enemy effective interception using encryption codes. Digital codes, number of keys, special features and security grade are some of the factors considered to grade communication security. This is, therefore, a subjective evaluation = 0.0 - 1.0

d. Nuclear Electromagnetic Pulse Protection

Specially fabricated components, inclusion of protective circuitry, and elaborate arrangement to ground the equipment will enable it to survive in a nuclear warfare (NW) environment:

(1) Complete protection = 1.0

(2) Partial protection = 0.5 - 0.0

e. Design Parameters

Good design parameters would facilitate the maintainability, transportability and logistic supportability of the system, keeping in view the diverse nature of weather and terrain and type of operation. Lightweight, more rugged and modularly built systems, are certainly desired on the modern battlefield:

(1) Weight. Lighter systems are more favorable and the evaluation criterion is subjective: 0.0 - 1.0

(2) Ruggedness. Owing to a lot of movement by varying means, the more rugged the equipment, the longer its life and enhanced reliability. The evaluation criterion is subjective: 0.0 - 1.0

(3) Modularity. Modularity in design makes the maintenance and repair of the system extremely easy and, hence, minimizes the mean time spent on repair:

Complete modular design = 1.0

Partial modular design = 0.75 - 0.0

(4) Standardization. It allows lower cost due to sharing of components within the system configurations and with those already existing systems which are compatible. The evaluation is subjective: 0.0 - 1.0

f. Repair and Maintenance

A good system design coupled with built in test facility would greatly reduce the time to repair:

(1) Built-in Test (BIT / BITE).

(a) System having BIT / BITE = 1.0

(b) System not having BIT / BITE = 0.0

(2) Mean Time Between Failure (MTBF).

(a) Mean Time Between Failure (MTBF), more than or equal to 1250 hours = 1.0

(b) MTBF between 900 and 400 hours = 0.75 - 0.5

(c) MTBF less than 400 hours = 0.25 - 0.0

(3) Mean Time To Field Repair (MTTFR).

(a) MTTFR less than or equal to one hour = 1.0

(b) MTTFR between 1 - 3 hours = 0.75 - 0.5

(c) MTTRF greater than 3 hours = 0.25 - 0.0

(4) Upgradability / Add-on Capability.

A well designed system will allow system modification and upgrading while maintaining its original design in order to meet the challenges of the adversary's future EW advancement. This factor will also enable the system to remain cost effective and current for a longer time.

Evaluation criterion is subjective and is a function of the type and degree of upgradability: 0.0 - 1.0

(5) Human Factors.

The system evaluation from the user point of view, e.g., simplicity of operation, accessibility and legibility of controls and displays, personal safety, etc., is important and subjectively graded: 0.0 - 1.0

g. Environmental

The ˙litary systems are vulnerable to exposure of extreme environmental conditions, e.g., temperature, humidity, underwater immersion, etc. A good system should, therefore, be able to operate with undergraded performance in existing country-wide environmental conditions:

Evaluation is subjective and = 0.0 - 1.0

h. Compatibility / Interoperability

Since simultaneous induction of the system to replace the existing (old) system would be limited owing to economic constraints, therefore, the progressive induction approach while continuing to use the old system will be a better option. The FH system so proposed for induction should, therefore, be interoperable in non-ECCM mode with the existing communication system currently in use:

(1) Compatible / Interoperable system = 1.0

(2) Non-compatible / Non-interoperable system = 0.0

i. Electromagnetic Interference (EMI)

A good system's filtering circuit design would enable it to be co-sited in the same vehicle with insignificant mutual interference to other systems in proximity. The non-interference quality is extremely important in multiple combat net radios (CNR) operating in a common operational area (at brigade / divisional level):

(1) No EMI to / from any VHF / HF system in the same vehicle or in multiple CNR operation = 1.0

(2) EMI experienced, but can be managed by improvisation = 0.5

(3) Significant EMI, difficult to overcome = 0.0

j. Transportability

Transportability, which mainly depends on the physical structure of the system, is more significant at the tactical level in varying terrain and weather conditions. The various versions, e.g., hand-held, man-pack, jeep-mounted, tank-fitted, etc., will afford greater system flexibility and favor human engineering:

(1) System transportable in all operations of war in all weather and terrain conditions = 1.0

(2) System posing some sort of difficulty in transportation = 0.5 - 0.0

3. System Evaluation Summary

Based on the criteria, three systems were chosen: Thomson-CSF PR4G, Tadiran CNR-900, and ITT Singars. Table 1 summarizes the comparative evaluation of the system parameters included in the MOE list as per paragraph 2 above. Table 2 includes only those parameters for which the information was available about all the three systems. Table 3 presents those parameters which could not be compared because information for one of the systems under consideration was not available.

TABLE 1

SYSTEM EVALUATION SUMMARY

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
GENERAL CHARACTERISTICS												
FREQUENCY COVERAGE	30-88MHz	1	1	1	30-88MHz	1	1	1	30-MHz	1	1	1
NUMBER OF AVAILABLE CHANNELS	2320	1	1	1	2320	1	1	1	2320	1	1	1
MODES OF OPERATION	CLEAR, COMSEC, & ECCM	1	1	1	CLEAR, COMSEC, & ECCM	1	1	1	CLEAR, COMSEC, & ECCM	1	1	1
POWER SOURCE	COMPATIBLE	1	1	1	COMPATIBLE	1	1	1	COMPATIBLE	1	1	1
POWER OUTPUT	0.4,4, & 40 W	1	1	1	0.25,4 & 50 W	1	1	1	4-50 W 3 STEPS	1	1	1
COMBAT NET RADIO	7 MEMOR-IZED NETS	1	1	1	10 MEMOR-IZED NETS	1	1	1	6 MEMOR-IZED NETS	.75	1	.75
REMOTE CONTROL OPERATION	<1.5 KMs	.75	1	.75	UP TO 4 KMs	1	1	1	@			
AUTOMATIC RETRANSMISSION	PROVIDED	1	1	1	PROVIDED	1	1	1	PROVIDED	1	1	1

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE
@ = NOT ENOUGH INFORMATION PROVIDED BY CONTRACTOR

TABLE 1 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
ANTI-JAM / ECCM PERFORMANCE												
HOPPING RATE	FAST TO MEDIUM	1	6	6	MEDIUM	0.75	6	4.5	MEDIUM	0.75	6	4.5
NUMBER OF PRESET CHANNELS	7	1	4	4	10	1	4	4	6	0.6	4	2.4
NUMBER OF PRESET FREQUENCY TABLES	16	1	4	4	10	1	4	4	@			
SYNCHRONIZATION	AUTO	1	5	5	AUTO	1	5	5	AUTO	1	5	5
ORTHOGONALITY	@				4 SETS OF 64 NETS	1	4	4	@			
<u>LOADING OF KEYS / FREQUENCY PLANS</u>. 1. SPEED AND EASE IN LOADING 2. TRANSEC OF KEYS	AUTO SECURE	1 1	3 3	3 3	AUTO SECURE	1 1	3 3	3 3	SEMI-AUTO SECURE	0.5 1	3 3	1.5 3
ERASING OF KEYS	PUSH BUTTON	1	6	6	OTHER MEANS	0.75	6	4.5	OTHER MEANS	0.5	6	3.0
FREE CHANNEL SEARCH	YES	1	5	5	NO	0	5	0	NO	0	5	0

*<u>KEY</u>.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE
@ = NOT ENOUGH INFORMATION PROVIDED BY CONTRACTOR

TABLE 1 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
COMMUNICATION SECURITY												
DIGITAL CODES, NUMBER OF KEYS ETC	SUBJECTIVE	1	5	5	SUBJECTIVE	0.5	5	2.5	SUBJECTIVE	0.5	5	2.5
NUCLEAR ELECTROMAGNETIC PULSE (NEMP) PROTECTION												
NEMP PROTECTION CIRCUITS ETC	COMPLETE FOR ALL PORTS	1	3	3	PARTIALLY DONE	0.5	3	1.5	PARTIALLY DONE	0.5	3	1.5
DESIGN PARAMETERS												
WEIGHT	SUBJECTIVE	1	4	4	SUBJECTIVE	.75	4	3	SUBJECTIVE	0.5	4	2
RUGGEDNESS	GOOD	1	3	3	GOOD	1	3	3	GOOD	1	3	3
MODULARITY	ALL	1	4	4	PARTIAL	.75	4	3	PARTIAL	.75	4	3
STANDARDIZATION	SUBJECTIVE	1	2	2	@				@			

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE
@ = NOT ENOUGH INFORMATION PROVIDED BY CONTRACTOR

TABLE 1 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
REPAIR AND MAINTENANCE												
BIT / BITE	YES	1	2	2	YES	1	2	2	YES	1	2	2
MTBF	@				4000	1	2	2	@			
MTTFR	@				LOW	1	2	2	@			
UPGRADABILITY / ADD-ON												
ADAPTIVE ANTENNAS, TDMA AND BURST MODE, INTERFACING WITH EXISTING / PROPOSED SYSTEMS	YES, PROGRAM IN HAND	1	6	6	NOT SPECI-FIC	0.5	6	3	NO PROGRAM GIVEN	0	6	0
HUMAN FACTORS												
EASE OF OPERATION, DISPLAYS AND CONTROLS	SUBJECTIVE	.75	2	1.5	SUBJECTIVE	1	2	2	SUBJECTIVE	.75	2	1.5

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE
@ = NOT ENOUGH INFORMATION PROVIDED BY CONTRACTOR

TABLE 1 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
COMPATIBILITY / INTEROPERABILITY												
WITH EXISTING VHF SYSTEM	YES	1	3	3	YES	1	3	3	YES	1	3	3
ELECTROMAGNETIC INTERFERENCE (EMI)												
WITHIN THE SAME VEHICLE, IN PROXIMITY OR CO-SITING	VERY LOW	1	3	3	LOW	0.5	3	1.5	LOW	0.5	3	1.5
TRANSPORTABILITY												
MANPACK, HANDHELD AND VEHICULAR	GOOD	1	1	1	GOOD	1	1	1	GOOD	1	1	1
TOTAL SCORE				81.25				69.5				47.15

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE
@ = NOT ENOUGH INFORMATION PROVIDED BY CONTRACTOR

TABLE 2

SUPPLEMENTARY SYSTEM EVALUATION SUMMARY

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
GENERAL CHARACTERISTICS												
FREQUENCY COVERAGE	30-88MHz	1	1	1	30-88MHz	1	1	1	30-88MHz	1	1	1
NUMBER OF AVAILABLE CHANNELS	2320	1	1	1	2320	1	1	1	2320	1	1	1
MODES OF OPERATION	CLEAR, COMSEC, & ECCM	1	1	1	CLEAR, COMSEC, & ECCM	1	1	1	CLEAR, COMSEC, & ECCM	1	1	1
POWER SOURCE	COMPATIBLE	1	1	1	COMPATIBLE	1	1	1	COMPATIBLE	1	1	1
POWER OUTPUT	0.4,4,& 40 W	1	1	1	0.25,4 & 50 W	1	1	1	4-50 W 3 STEPS	1	1	1
COMBAT NET RADIO	7 MEMORIZED NETS	1	1	1	10 MEMOR-IZED NETS	1	1	1	6 MEMOR-IZED	.75	1	.75
AUTOMATIC RETRANSMISSION	PROVIDED	1	1	1	PROVIDED	1	1	1	PROVIDED	1	1	1

*KEY.
A = PARAMETER VALUE   B = SCORE   C = WEIGHTING FACTOR   D = A*B = TOTAL PARAMETER SCORE

TABLE 2 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
ANTI-JAM / ECCM PERFORMANCE												
HOPPING RATE	FAST TO MEDIUM	1	6	6	MEDIUM	0.75	6	4.5	MEDIUM	0.75	6	4.5
NUMBER OF PRESET CHANNELS	7	1	4	4	10	1	4	4	6	0.6	4	2.4
SYNCHRONIZATION	AUTO	1	5	5	AUTO	1	5	5	AUTO	1	5	5
LOADING OF KEYS / FREQUENCY PLANS 1. SPEED AND EASE IN LOADING 2. TRANSEC OF KEYS	AUTO SECURE	1 1	3 3	3 3	AUTO SECURE	1 1	3 3	3 3	SEMI-AUTO SECURE	0.5 1	3 3	1.5 3
ERASING OF KEYS	PUSH BUTTON	1	6	6	OTHER MEANS	0.75	6	4.5	OTHER MEANS	0.5	6	3.0
FREE CHANNEL SEARCH	YES	1	5	5	NO	0	5	0	NO	0	5	0

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE

TABLE 2 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
COMMUNICATION SECURITY												
DIGITAL CODES, NUMBER OF KEYS ETC	SUBJECTIVE	1	5	5	SUBJECTIVE	0.5	5	2.5	SUBJECTIVE	0.5	5	2.5
NUCLEAR ELECTROMAGNETIC PULSE (NEMP) PROTECTION												
NEMP PROTECTION CIRCUITS ETC	COMPLETE FOR ALL PORTS	1	3	3	PARTIALLY DONE	0.5	3	1.5	PARTIALLY DONE	0.5	3	1.5
DESIGN PARAMETERS												
WEIGHT	SUBJECTIVE	1	4	4	SUBJECTIVE	.75	4	3	SUBJECTIVE	0.5	4	2
RUGGEDNESS	GOOD	1	3	3	GOOD	1	3	3	GOOD	1	3	3
MODULARITY	ALL	1	4	4	PARTIAL	.75	4	3	PARTIAL	.75	4	3

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE

TABLE 2 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
REPAIR AND MAINTENANCE												
BIT / BITE	YES	1	2	2	YES	1	2	2	YES	1	2	2
UPGRADABILITY / ADD-ON												
ADAPTIVE ANTENNAS, TDMA AND BURST MODE, INTERFACING WITH EXISTING / PROPOSED SYSTEMS	YES, PROGRAM IN HAND	1	6	6	NOT SPECIFIC	0.5	6	3	NO PROGRAM GIVEN	0	6	0
HUMAN FACTORS												
EASE OF OPERATION, DISPLAYS AND CONTROLS	SUBJECTIVE	.75	2	1.5	SUBJECTIVE	1	2	2	SUBJECTIVE	.75	2	1.5

*KEY.
A = PARAMETER VALUE B = SCORE C = WEIGHTING FACTOR D = A*B = TOTAL PARAMETER SCORE

TABLE 2 (CONTINUED)

SYSTEM PARAMETERS	THOMSON-CSF PR4G SYSTEM				TADIRAN CNR-900 SYSTEM				ITT SINCGARS SYSTEM			
	*A	*B	*C	*D	*A	*B	*C	*D	*A	*B	*C	*D
COMPATIBILITY / INTEROPERABILITY												
WITH EXISTING VHF SYSTEM	YES	1	3	3	YES	1	3	3	YES	1	3	3
ELECTROMAGNETIC INTERFERENCE (EMI)												
WITHIN THE SAME VEHICLE, IN PROXIMITY OR CO-SITING	VERY LOW	1	3	3	LOW	0.5	3	1.5	LOW	0.5	3	1.5
TRANSPORTABILITY												
MANPACK, HANDHELD AND VEHICULAR	GOOD	1	1	1	GOOD	1	1	1	GOOD	1	1	1
TOTAL SCORE				74.5				56.5				47.15

*KEY.
A = PARAMETER VALUE   B = SCORE   C = WEIGHTING FACTOR   D = A*B = TOTAL PARAMETER SCORE

TABLE 3

SUMMARY OF PARAMETERS FOR WHICH ENOUGH INFORMATION WAS NOT AVAILABLE

PARAMETER	SYSTEM
REMOTE CONTROL OPERATION	ITT SINCGARS SYSTEM
NUMBER OF PRESET FREQUENCY TABLES	ITT SINCGARS SYSTEM
ORTHOGONALITY	THOMSON-CSF PR4G AND ITT SINCGARS SYSTEMS
MTBF	THOMSON-CSF PR4G AND ITT SINCGARS SYSTEMS
MTTFR	THOMSON-CSF PR4G AND ITT SINCGARS SYSTEMS

D. SYSTEM EVALUATION BASED ON FIELD TRIALS, DENDRITIC APPROACH (SIMILAR TO OT&E)

1. General

Operation test and evaluation (OT&E) of a system is conducted by the user organization duly assisted by the combat support and combat service support elements. It must be done in the most realistic combat simulated environments. For a FH CNR system, the one considered here, realism would be created by simulating intense EW activity, e.g., jamming (all types), direction finding, intercepting, etc. The key features of performance, namely anti-jamming, co-location and man-machine-interface, are keenly observed. The conduct of T&E should be preferably planned in such a way that those personnel operating, maintaining and repairing the equipment, when fielded, must all be included in the T&E team. The proposed test team organization is given in Figure 10.

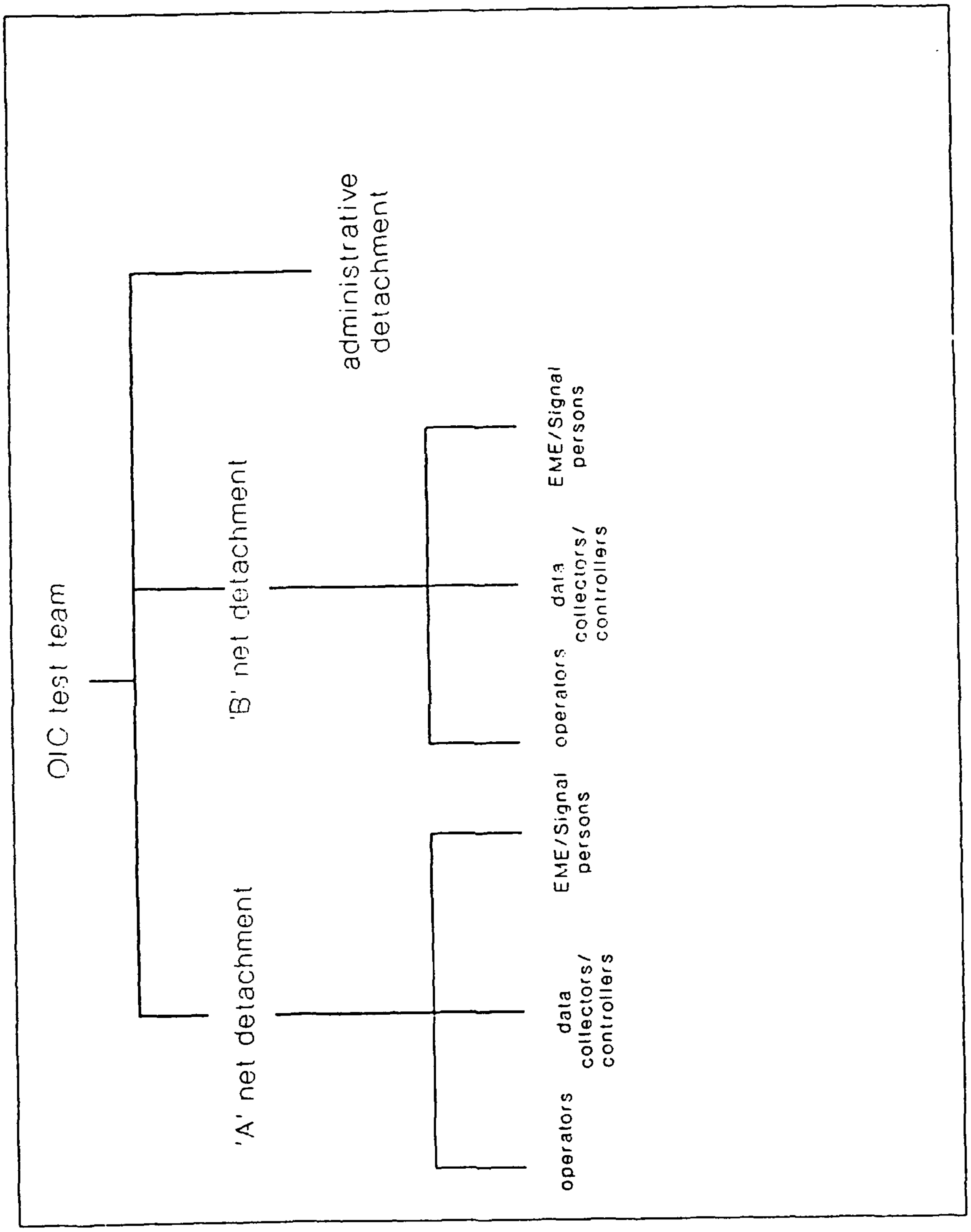


Figure 10

Organization Of OT&E Team

The initial OT&E may be conducted by a battalion level task force with subsequent expansion to a brigade and division level. The most preferable course of action may be to integrate the T&E with field training exercises already planned.

2. OT&E Objectives

a. To evaluate the operational effectiveness and operational suitability of a typical frequency hopping communication system with particular emphasis to anti-jam performance.

b. To provide information on organization, personnel requirements, doctrine and tactics [Ref. 6].

c. To verify manufacturer's specifications, operating instructions, software documentation, publications and handbooks [Ref. 6].

3. Critical Issues

a. Anti-jamming performance: Is the system resistant enough to enemy jamming effort (all types repeat, narrowband and barrage) in order to provide command and control communication at the tactical level?

b. Logistic supportability: Will a country like Pakistan be able to maintain an efficient chain of logistic echelon (repair and maintenance) based on its own indigenous resources of men and material while keeping in mind cost effectiveness?

c. Interoperability: In order to ensure progressive induction of the equipment on a priority basis, is it compatible with the existing VHF tactical communication radios?

d. Upgradability: Keeping in mind the future needs of the modern battlefield command, control, communication and weapon systems, will it allow interfacing and adding-on of other sub-systems?

e. Electromagnetic Interference (EMI) and Co-siting. To check the system performance, keeping in mind the military standards as per the current manual on the subject and seek answers to the following questions:

1. What is the quality of communication (voice / data) when other nets (about 4 to 5 in number) using same / different systems operate simultaneously?

2. How much interference does it create in other systems in the proximity (located in the same vehicle / in local area within a radius on 3 to 4 Km)?

3. How much interference does it receive when working in close proximity with the other systems?

4. Evaluation Criteria / Measure of Effectiveness

The thresholds and measures of effectiveness (MOEs) as shown in Table 4 will be taken as guidelines, and greater emphasis shall be laid on the operational performance for each test. The laboratory tests obviously will be more quantifiable, however, operational tests will be mission-effectiveness oriented. The integration of these test results would, therefore, pay dividends.

TABLE 4

EVALUATION CRITERIA / MOEs

TEST DESCRIPTION	MOE / THRESHOLD
Anti-jamming	Voice comm; sig str= 5/5, BER = 1/1000 Data comm; BER = 1/100000
EMI / Co-siting	As per EMI tech manual
Operational Availability	Ao of 90% without add-on eqpt Ao of 85% with add-on eqpt
Reliability	MTBF > 1550 hours for normal mode = > 1250 hours for FH mode
Maintainability (field repairs)	MTTFR =< 0.5 hours (including BIT)
Interoperability	Subjective
Upgradability	Subjective

5. Essential Elements of Analysis (EEA) / Dendritic Approach

The test objectives with greater emphasis on critical issues are best addressed by adopting the dendritic approach as shown in Figures 11-15.

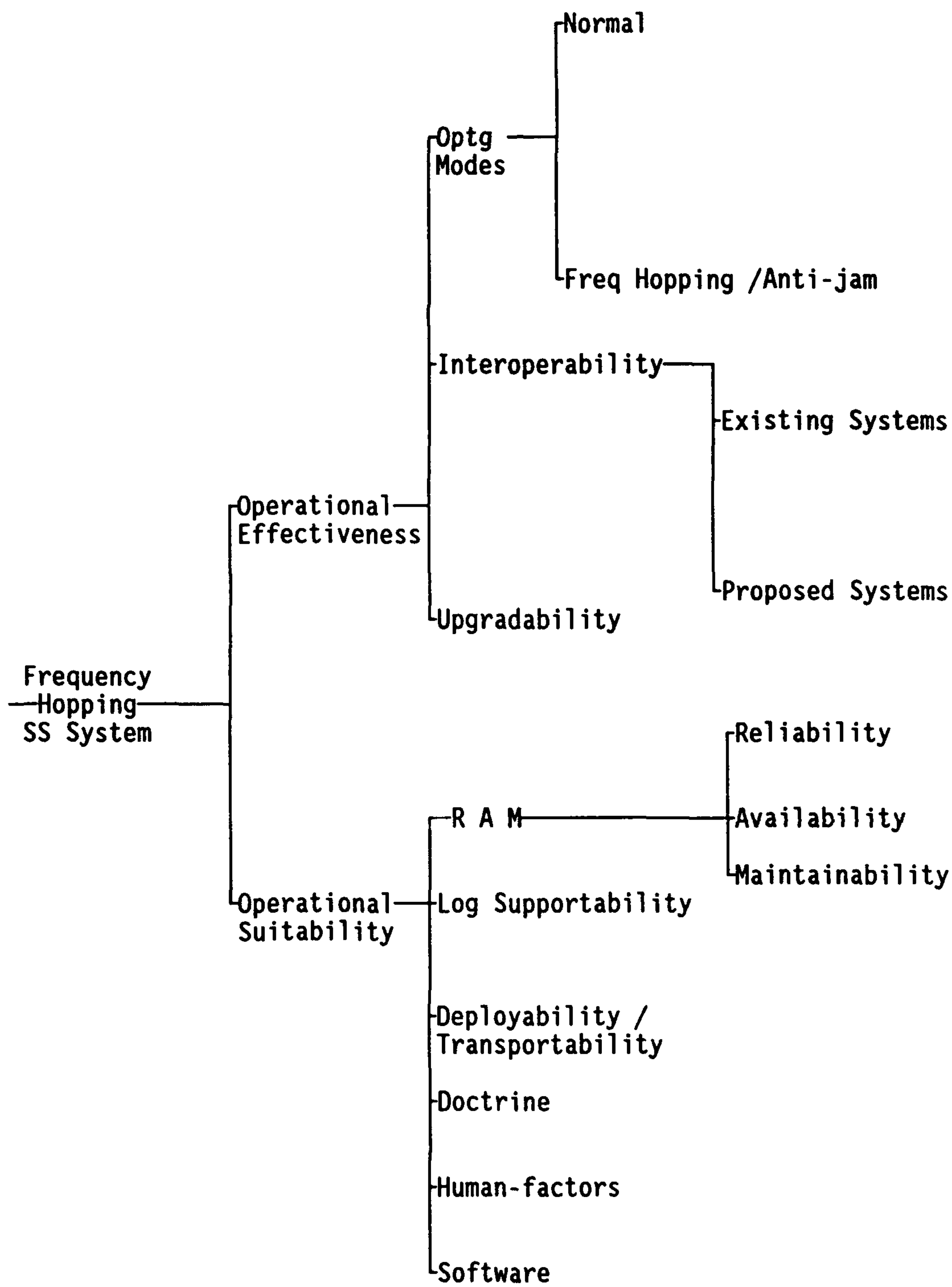


Figure 11

Master Dendritic Of Frequency Hopping Spread Spectrum System

- Freq Hopping Anti-jam Performance
  - Single net (min 5 sub-stations)
    - Under jamming condition
      - Data comm
        - *BER ?
        - *Auto Correction Codes ?
        - *comm Range ?
      - Voice comm
        - *Signal Strength ?
        - *Comm Range ?
    - Under no jamming (voice & data)
      - *Comm range ?
      - *BER ?
      - *Signal Strength ?
  - Mutiple Nets (min 4 nets)
    - Using same system under jamming conditions $\boxed{*,@}$
    - Using different systems under jamming conditions $\boxed{*,@}$

<u>Key</u>

* Performance checked under all weather & terrain conditions

@ Performance checked for mutual interference (freq management, BER, signal strength)

Figure 12

Partial Dendritic For Anti-jamming Performance Of Frequency Hopping Spread Spectrum System

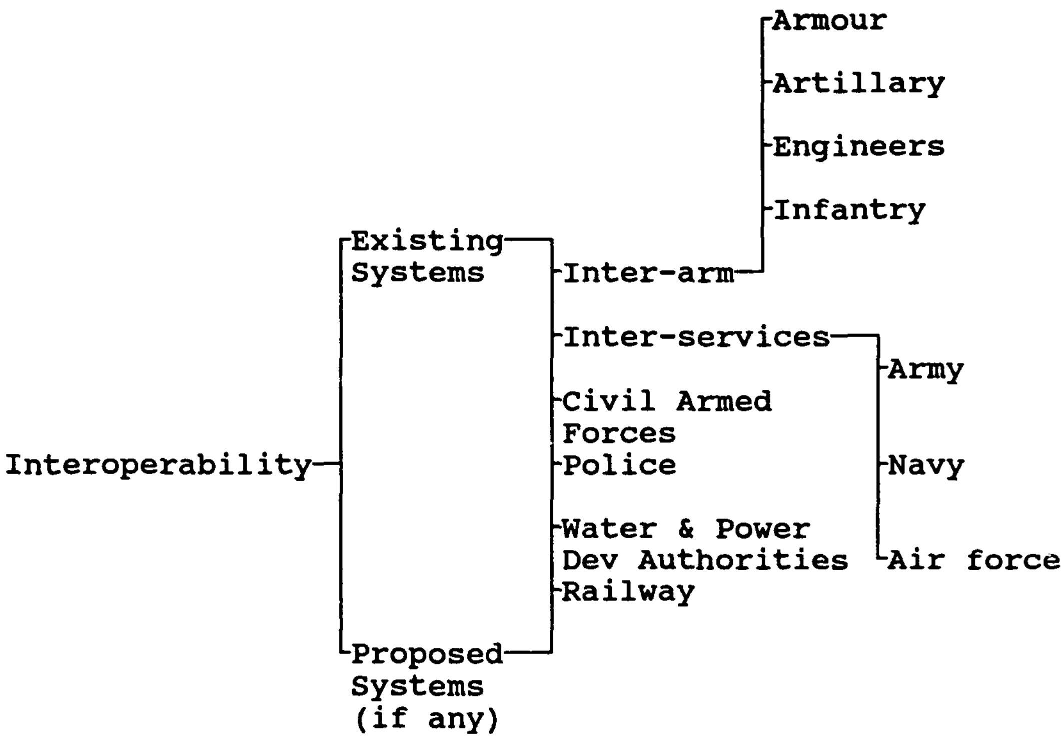


Figure 13

Partial Dendritic Of Interoperability For Frequency Hopping System

Upgradability/Add-on (Software / Hardware)
- Bulk Secrecy Equipment
- Burst Communication Equipment
- Computer Network
- Data Communication
- Satellite Communication
- Null Steering Antenna

Figure 14

Partial Dendritic Of Upgradability / Add-on For Frequency Hopping System

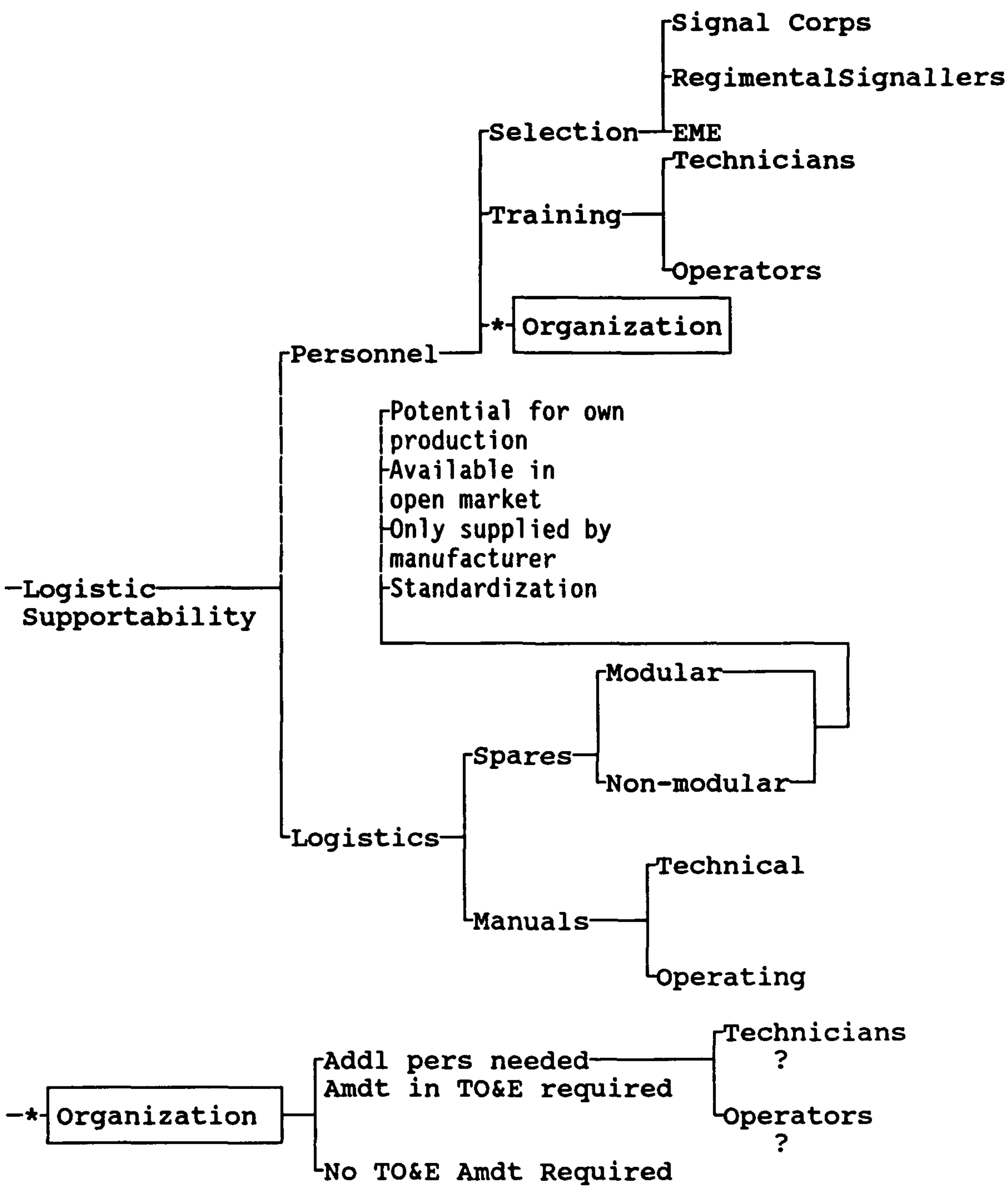


Figure 15

Partial Dendritic Of Logistic Supportability For Frequency Hopping System

E. LIMITATIONS

The OT&E work done in this paper is certainly not inclusive of all the aspects of evaluation, rather it serves as a guideline for a more in-depth evaluation and analysis process. Following are some the limitations of the evaluation done for the system under consideration:

1. Field trials could not be conducted due to paucity of time and non-availability of equipment and manpower.

2. The OT&E detailed information could not be provided due to security classification of the subject area.

3. The detailed EEA is not dealt with as it is beyond the scope of the thesis.

4. The results of DT&E and OT&Es (done by other sources) could not be included / consulted due to their non-availability.

5. Simulation could not be do · · due to lack of time and scope of the work.

6. The comparative evaluation is based on the specifications. At this stage it may not be verified by other sources / means.

7. Some of the specifications have to be graded subjectively due to non-availability of their exact values.

8. One of the most important considerations is the comparative cost-effectiveness of the systems (the initial and the subsequent spares cost) which could not done, as such information was not provided by the vendors.

VI. CONCLUSIONS AND RECOMMENDATIONS

The conventional combat net control radios currently held in the inventory cannot provide survivable communication under the existing EW threat scenario. Therefore, a more sophisticated combat net radio system capable of providing security, covertness and anti-jamming ought to be fielded. With modern technology at hand, frequency hopping combat net radio is by far the best and most practically tested system.

One of the most important factors which must never be lost sight of is the enemy's EW capabilities. They must be accurately gauged and analyzed. Under an adequately potent EW threat scenario, slow frequency hopping combat net radios will be highly vulnerable, especially to spot jamming. The quality of voice communication using medium frequency hopping CNR would also be degraded significantly. Barrage jamming could be more effective, but it would require huge power density, which may become a remote option adopted by the enemy.

The most effective type of jamming employed against a working CNR, would be repeat / follower jamming. Under the present threat scenario, it is probably safe enough to use a fast frequency hopping CNR. A fast frequency hopper will provide greater processing gain, more jamming margin, and less time of reaction for any effective hostile counter measures. It will, however, remain a battle of achieving high speeds of signal processing, on both sides, using VLSI circuits, surface-mounted components, and microprocessors.

Frequency hopping systems are comparatively more vulnerable to detection and subsequent direction finding. This will certainly increase the chances of destruction of own systems by the hostile bombardment and commando actions / raids. Moreover, it will also leak out some combat intelligence about the layout, pattern and extent of friendly forces deployment.

Direct sequence spread spectrum signals have more inherited covertness but lack one of the fundamental performance features of "co-location". Therefore, its employment in a CNR system is precluded. However, direct sequence systems have far greater potential applications in point-to-point radio links. The area of using direct sequence in combination with other techniques, e.g., frequency hopping, is currently under intensive research, and much of the work is classified.

As regards the system evaluation of specific systems considered for this thesis work, the Thomson-CSF PR4G system has shown greater promise as compared to the other two systems. It, therefore, is a good candidate for fielding in the Pakistan Army,s tactical level CNR communications. The most significant features of the Thomson-CSF PR4G system include its anti-jam capability (especially fast to medium hopping rate) and add-on / upgradability. Other significant features of Thomson-CSF PR4G include more number of preset frequency tables, push button erasing of frequency keys, digital codes, and free channel search. The upgradability program of the PR4G system with regard to the adaptive antenna, burst transmission, multi channel TDMA, and interfacing with existing / proposed data networks will increase the system life span.

APPENDIX A

LIST OF MANUFACTURERS

Thomson-CSF (France),

Division Telecommunications-66,

rue du Fosse Blanc-B.P.30-92231

Gennevilliers Cedex France.

Phone: (33-1)47.91.80.00

Telex: TCSFDTC 62084

Tadiran (Israel),

11 Ben-Gurion St. Givat Shmuel 51905, Israel.

Phone: (972-3)713111

Tlx: 341492,33537

Fax: (972-3)713721

Marconi (UK), Secure Radio,

Browns Lane, The Airport, Portsmouth,

Hamshire, England, PO35PH.

Phone: 44-1705674368

: (0705)664966

Fax: 44-1705672934

Telex: 869442

: 869442

Magnavox (USA),

1313 Production Road, Fort Wayne, IN 46808 USA.

Phone: (219)-429-6000

(219)-429-4178

Plessy (UK),

Plessy Military Communications Limited,

Ilford, Essex, United Kingdom IG14AQ.

Phone: 01-4783040

Telex: 897971

ITT (USA),

Aerospace / Optical Division

3700 East Pontiac Street, P.O Box 3700

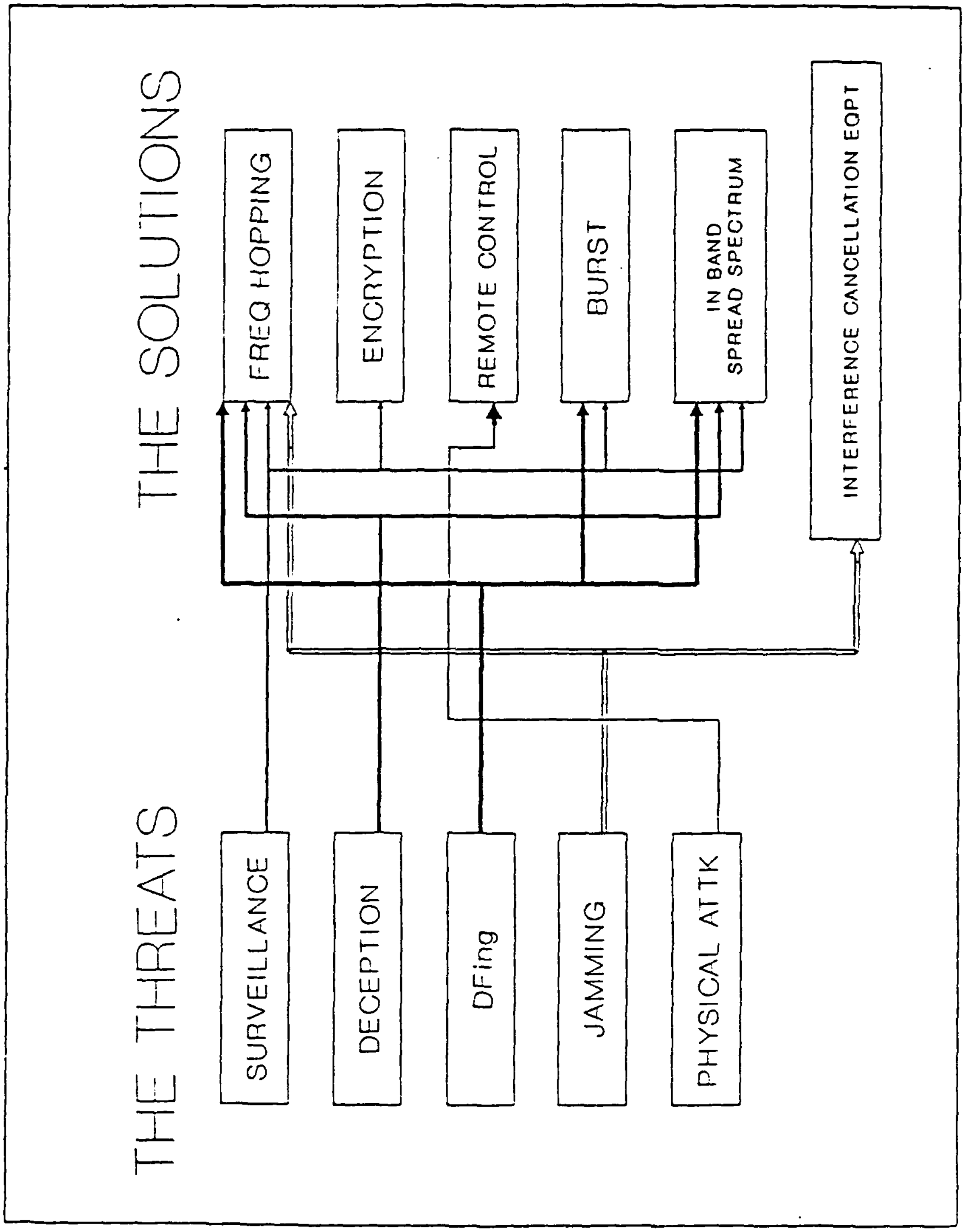
Fort Wayne, Indiana 46801 USA.

Telex: 23-24-29 TWX 810-332-1413

Phone: (219)-423-9636

APPENDIX B

LIKELY EW THREATS AND POSSIBLE SOLUTIONS



APPENDIX C

ACRONYMS AND ABBREVIATIONS

AJ	Anti-jamming
Amdt	Amendment
A_o	Operational Availability
Auto	Automatic
BPSK	Biphase Phase Shift Keying
BER	Bit Error Rate
BIT	Built-In-Test
BITE	Built-In-Test Equipment
C^3	Command, Control and Communications
CDMA	Code Division Multiple Access
CNR	Combat Net Radio
Comm	Communication
COMSEC	Communication Security
CW	Continuous Wave
dB	Decibel(s)
Dev	Development
DF/DFing	Direction Finding
DS	Direct Sequence/Direct Spreading
DSSS	Direct Sequence Spread Spectrum System
DT&E	Development Test and Evaluation
ECM	Electronic Counter Measures
ECCM	Electronic Counter-Counter-Measures
EEA	Essential Elements of Analysis

ELINT	Electronic Intelligence
EMCON	Emission Control
EME	Electrical Mechanical Engineers
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
ESM	Electronic Support Measures
EW	Electronic Warfare
F_b	Information Frequency
FOO	Forward Observation Officer
Freq	Frequency
f_c	Chip Frequency
Fhop	Hopping Frequency
Flo	Frequency of Local Oscillator
FH	Frequency Hopping
FM	Frequency Modulation
FSK	Frequency Shift Keying
HF2	High Frequency
Hz	Hertz
KM	Kilometers
IF	Intermediate Frequency
LO	Local Oscillator
LPI	Low Probability of Intercept
LPE	Low Probability of Exploitation
LPPF	Low Probability of Position Fix
MOE	Measure Of Effectiveness
MTBF	Mean Time Between Failure

MTTFR	Mean Time To Field Repair
OIC	Officer In Charge
Op	Operation/operator
Optg	Operating
OT&E	Operation Test and Evaluation
PSK	Phase Shift Keying
PN	Pseudorandom Noise, Pseudonoise, Pseudorandom Sequence
QPSK	Quadraphase Phase Shift Keying
RF	Radio Frequency
Rx	Receiver
Regtl	Regimental
RAM	Reliability, Availability and Maintainability
ROC	Required Operational Capabilities
Sec	Seconds
Sig	Signal
SIGINT	Signal Intelligence
S/J	Signal to Jamming Ratio
S/N	Signal to Noise Ratio
Sqn	Squadron
SS	Spread Spectrum
SSS	Spread Spectrum System
TH	Time Hopping
T&E	Test And Evaluation
TO&E	Table Of Organization And Equipment
TRANSEC	Transmission Security

Tx	Transmitter
TOA	Time of Arrival
VCO	Voltage Controlled Oscillator
VHF	Very High Frequency
W	Watt(s)

APPENDIX D

GLOSSARY OF TERMS

Autocorrelation

The measure of similarity in the amplitude and phase of a signal or code and a time delay replica of itself. In an SS system, the autocorrelation of a spreading code with a delayed replica of itself is of prime importance. The amount of similarity in this case is the number of bits that are similar (agreements) minus the number of bits that are different (disagreements) between the original sequence and the time delayed replica. [Ref. 3]

Base band

The original information band before modulation of a carrier. An audio band from a microphone used to modulate a carrier is an example of a base band. [Ref. 2]

Baud

A unit of signalling speed indicating the number of code elements generated per second. In SS systems, baud is used when referring to the rate at which the information or traffic is being generated. [Ref. 3]

Baud rate

Baud rate is often used instead of baud. However, the correct term for the signalling speed is baud and not baud rate. [Ref. 3]

Biphase Phase Shift Keying (BPSK)

A phase shift keyed signal in which the phase changes in increments of 180 degrees. BPSK is often used for generating a DS, SS signal. [Ref. 3]

Chip

In SS systems, a chip is a single element of a spreading code. A chip may consist of one or more bits, depending on the application. For example, a chip is a single bit for a biphase DS signal, whereas a chip consists of two bits for a quadraphase signal. Two bits are required in the quadra-phase signal to control the four carrier phases, e.g., 00 for 0^0, 01 for 90^0, 11 for 180^0, and 10 for 270^0. [Ref. 3]

Co-siting / Co-location

A very important characteristic of tactical radios (particularly the vehicular mounted versions). This implies that for a CNR it must be possible to operate two or more transceivers belonging to different networks and placed in close proximity of each other, and/or of other radiating equipment (such as radars), without the result being a babble of mutual interference and background noise.

Chip rate

The number of chips or code elements per second generated by the spreading code generator of a SS signal. Chip rate and baud are both measurements of signalling speeds denoting the number of code elements generated per second. Baud is generally used when referring to the traffic, or information, and chip is used when referring to the spreading code. [Ref. 3]

Communication Security (COMSEC)

Consists of physical security, cryptosecurity, transmission security, and emission security. [Ref. 7]

Coherence

The condition when a received signal and a receiver's reference are synchronized and in phase. [Ref. 3]

Correlation

The measure of similarity of two signals. The similarity is generally based on the amplitude and phase of the signals. A correlation peak indicates a maximum amount of similarity in amplitude and phase. [Ref. 3]

Cross-Correlation

The measure of similarity between any two signals. In SS systems, cross-correlation is used to determine whether or not the received signals contain the desired coded signal, e.g, correlating the received signals with a receiver-generated code replica signal. [Ref. 3]

Direction Finding

A procedure used for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. It is a useful intelligence aid to find out the enemy force's deployment pattern and extent.

Emission Security

The term usually associated with such effort is TEMPEST, which refers to investigations and studies of compromising and inadvertent emanations. An example of a compromising situation is one where the input signal into a cryptographic unit provides enough leakage to be detected. [Ref. 7]

Electronic Counter Measures (ECM)

That branch of EW which deals with the actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. ECM includes:

1. Jamming. It involves deliberate reradiation or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by the enemy. Spot jamming is done against a specific frequency or channel. Barrage jamming is done against a band of frequencies. If barrage jamming is done with a noise-like signal moving rapidly and irregularly, then it is known as sweep jamming. If the jamming is made agile in frequency and time, following the same PN sequence as that of the victim, then it is known as following / repeat jamming. This is one of the most effective ways of jamming. In it, the threat signal is received by the ESM system, processed in real time, and retransmitted along with noise. For the effective-ness of this type of jamming, the time spent by the ESM and ECM systems in receiving, processing, and retransmission must be less than the hopping rate of the victim system.

2. Deception. It deals with the deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead the enemy in the interpretation or use of information received by his electronic systems. There are two categories of deception: [Ref. 7]

a. Manipulative. The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

b. Imitative. Deals with introducing radiation into hostile channels which imitates his own emissions.

Frequency Management

To avoid EMI / co-siting problems, one of the most important factors is the assignment of frequencies to nets at various tactical levels. In most of the state-of-the-art FH CNR systems, frequency allotment is done using highly efficient algorithms.

Free Channel Search (FSR)

A very important feature of an FH radio which enables a network frequency selection outside the jammed bands for the duration of push-to-talk.

Interference Cancellation (ICE) Equipment

A radio equipped with ICE equipment will greatly reduce the effects of jamming. This is done by electronically steering a null in the receiving station antenna, thus counteracting the strongest unwanted signals.

In order to produce covertness by using ICE, a friendly jammer is integrated into the active radio net, thereby letting the enemy receive strong jamming signals. This at the same time will not affect the active net as it will cancel out own-jammer strong signals.

Hopping rate

The rate at which the carrier frequency is changed in a FH system. The hopping rate is defined as: [Ref. 3]

Hopping Rate = 1 / dwell time at a given RF.

In general, hopping rate is some multiple of the baud.

Modulo-2 addition

An arithmetic addition of binary digits. Logic gates that perform this function are called Exclusive-OR gates. Examples of the addition are: [Ref. 3]

$$0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1,\ 1 + 1 = 0$$

Multipath

A phenomenon where the signal reaches the receiving antenna from two or more paths (usually a direct and indirect path). The two signals may enhance or cancel one another depending on the relative amplitudes and phases.

Near-Far Performance

Near-far performance describes the interaction of spread spectrum systems with other users both near and far away from the intended users. A frequency hopping system jumps to many different carrier frequencies in a time interval and filters the carrier frequencies with IF filters. Users outside the bandwidth are rejected, and only the proper signal is demodulated. Since the IF filter passes only a narrow bandwidth signal, potential interferers are more easily rejected. [Ref. 3]

If some users of the frequency band are near the frequency hop receiver and the frequency hop transmitter is far away, a frequency hop system can more easily reject the nearby interference than the direct sequence system can.

Orthogonal

This term is widely used for the following applications:

1. In statistics, for statistical independence.
2. In algebra, for vectors perpendicular to each other.
3. In coding theory, for describing a set of codes that have zero cross-correlation coefficients for all pairs in the set.

Orthogonal FH

A modulation scheme that allows two or more FH schemes to work at the same frequencies without interfering with one another. The timing of the FH of each system is synchronized in such a way that they never transmit on the same frequency at the same time.

Power Management

In order to protect friendly ESM receivers from damage owing to high power influx and at the same time ensure required output powers for communication, it is essential that power management, or in other words proper power allocation, has to be done.

Processing Gain and Jamming Margin

Processing gain (G_p) and one of its important derivatives, jamming margin (M_j), are two very important SSS parameters. They are quantitatively defined as: [Ref. 2]

For DS / FH SSS; $G_p = BW_{rf} / R_{info}$

$= f_c / f_b$

= number of frequency choices (for FH only)

where f_b and f_c are information and chip rates respectively.

For TH SSS; G_p = 1 / transmit duty cycle.

For chirp SSS; G_p = Compression ratio = D = $f_{sweep} * t_{sweep}$.

For all SSS; $M_j = G_p - \{ L_{sys} + (S / N)_{out} \}$

where L_{sys} = System implementation losses and $(S/N)_{out}$ = SNR at the information output.

Pseudonoise (PN)

A signal that appears to be noise before modulation (also called noise-like signal, pseudorandom noise, pseudorandom sequence). This term is very commonly used to describe the spreading code in SS systems. The PN, although having no apparent pattern, repeats itself after a long time interval. [Ref. 3]

Quadraphase Phase Shift Keying (QPSK)

It is a method in which the signal phase changes are made in multiples of 90^0. QPSK is commonly used to generate DS, SS signals.

Synchronization

The process of eliminating the time delays between a received sequence or signal and replica generated by the receiver.

Spoofing

The technique in which an unfriendly communication radio net emulates the friendly radio net and transmits erroneous orders or data in order to create chaos and confusion.

Signal Security

The protection of one's radiations from enemy SIGINT is called signal security (SIGSEC). SIGSEC involves both communication security (COMSEC) and electronic security (ELSEC). SIGSEC is to SIGINT as ECCM is to ECM. [Ref. 7]

Surveillance

One of the techniques used for intelligence gathering. Most obviously, plain messages may be intercepted. However, vital clues may be given to the enemy by signature recognition, type of modulation, operating procedures, or traffic statistics and the number and direction of transmitters.

Transmission Security

Transmission security (TRANSEC) is designed to protect transmissions from hostile interception and exploitation. This is achieved by using covert systems employing spread spectrum techniques and observing emission control (EMCON).

LIST OF REFERENCES

1. Myres, A. Glen, "Class Notes for EC4560: Communications ECCM," Naval Postgraduate School, June 1990.

2. Dixon, C. Robert, "Spread Spectrum Systems," A Wiley-Interscience Publication, John Wiley & Sons, New York, 1984.

3. Loomis, H. Herschel, "Class Notes for EO3780: EW Computer Applications," Naval Postgraduate School, June 1991.

4. Ziemer, R. E., and Peterson, R. L., "Digital Communications and Spread Spectrum Systems," Macmillan Publishing Co., New York, 1985.

5. Jordan, C. Edward, "Reference Data for Engineers: Radio, Electronics, Computer and Communications," Howard W. Sams and Company, A division of Macmillan, Inc., Indiana, 1989.

6. Nakagawa, Gordon R., "Class Notes for OS4601: Test and Evaluation," Naval Postgraduate School, June 1991.

7. Scheleher, D. Curtis, "Introduction to Electronic Warfare," Artech House, 1986.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Dan C. Boger, Code AS/Bo Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
4.	CDR Allan Tulloch, Code AS/Tu Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
5.	Electronic Warfare Directorate Naval Headquarters Islamabad Pakistan	1
6.	Commandant Military College of Signals Rawalpindi, Pakistan	2
7.	PAF Air HQ Islamabad, Pakistan	1
8.	Major Syed Agha Hussain Village Esa Khel-Kachai P.O. Landi-Kachai Tehsil and District Kohat, Pakistan	4